#5

Docket: 1232-4577 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Kurumi Mori

Serial No. : 09/412,900 Group Art Unit : 2766

Filed : October 5, 1999

For : INFORMATION COMMUNICATION APPARATUS AND METHOD, INFORMATION COMMUNICATION SYSTEM, AND MEMORY MEDIUM

ASSISTANT. COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

CLAIM TO CONVENTION PRIORITY

In the matter of the above-identified application and under the provisions of 35 U.S.C. §119 and 37 C.F.R. §1.55 applicants claim the benefit of the following prior applications:

Application Filed In:	Japan
Serial No.:	10-287774
Filing Date:	October 9, 1998

1. [X] Pursuant to the Claim to Priority, applicants submit duly certified copies of said foreign application.

2. [ ] A duly certified copy of said foreign application is in the file of application Serial No. ____, filed _____.

Respectfully submitted,
MORGAN & FINNEGAN

Dated: November 19, 1999

By: _____
Michael M. Murray
Registration No. 32,537

Mailing Address:
MORGAN & FINNEGAN
345 Park Avenue
New York, New York 10154

GP2766

Docket: 1232-4577

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Kurumi Mori

Serial No. : 09/412,900 Group Art Unit : 2766

Filed : October 5, 1999

For : INFORMATION COMMUNICATION APPARATUS AND METHOD, INFORMATION COMMUNICATION SYSTEM, AND MEMORY MEDIUM

CERTIFICATE OF MAILING (37 C.F.R. 1.8a)

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

I hereby certify that the attached Claim to Convention Priority; Certified Copy of Priority Document (JP 10-287774); and return receipt postcard (along with any paper(s) referred to as being attached or enclosed) and this Certificate of Mailing are being deposited with the United States Postal Service on the date shown below with sufficient postage as first-class mail in an envelope addressed to the: U.S. Patent and Trademark Office, Washington, DC 20231.

Respectfully submitted,

MORGAN & FINNEGAN, L.L.P.

By: _____
Michael M. Murray

Date: November 19, 1999

Mailing Address:
MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, New York 10154
(212) 758-4800
(212) 751-6849 Telecopier

CFO 13908 US/Y

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年１０月　９日

出願番号
Application Number: 平成１０年特許願第２８７７７４号

出願人
Applicant (s): キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年１０月２９日

特許庁長官
Commissioner,
Patent Office

近藤隆

【書類名】　特許願

【整理番号】　3666032

【提出日】　平成10年10月 9日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明の名称】　情報通信装置及び方法、情報通信システム、記録媒体

【請求項の数】　20

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

【氏名】　森　くる美

【特許出願人】

【識別番号】　000001007

【氏名又は名称】　キヤノン株式会社

【代理人】

【識別番号】　100090273

【弁理士】

【氏名又は名称】　國分　孝悦

【電話番号】　03-3590-8901

【手数料の表示】

【予納台帳番号】　035493

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705348

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報通信装置及び方法、情報通信システム、記録媒体

【特許請求の範囲】

【請求項１】　送信情報の暗号化手段と、

情報の通信を行う際に、上記暗号化手段の使用／不使用を選択する暗号処理選択手段とを備えたことを特徴とする情報通信装置。

【請求項２】　上記暗号処理選択手段は、上記送信情報の暗号化処理を行うかどうかを指示するための指示手段を備え、情報送信者からの指示に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１に記載の情報通信装置。

【請求項３】　上記暗号処理選択手段は、情報送信側の装置と情報受信側の装置とが接続されている通信媒体を判別する媒体判別手段を備え、接続されている通信媒体に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１に記載の情報通信装置。

【請求項４】　上記暗号処理選択手段は、情報受信側の装置において暗号解読が可能であるかどうかを判別する暗号許可判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１に記載の情報通信装置。

【請求項５】　上記暗号処理選択手段は、上記送信情報の機密度を判別する機密度判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１に記載の情報通信装置。

【請求項６】　受信情報が暗号化されているか否かを判別する暗号判別手段と、

上記暗号判別手段によって上記受信情報が暗号化されていると判別された場合に、所定のエラー処理を行うエラー処理手段とを備えたことを特徴とする情報通信装置。

【請求項７】　情報の通信を行う際に、送信情報の暗号化処理の使用／不使用を選択するようにしたことを特徴とする情報通信方法。

【請求項８】　情報送信者からの指示に応じて上記送信情報の暗号化処理の

使用／不使用を選択するようにしたことを特徴とする請求項７に記載の情報通信方法。

【請求項９】　情報送信側の装置と情報受信側の装置とが通信可能な異なる通信媒体のうち、使用している通信媒体に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしたことを特徴とする請求項７に記載の情報通信方法。

【請求項１０】　情報受信側の装置において暗号解読が可能であるかどうかの判別結果に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしたことを特徴とする請求項７に記載の情報通信方法。

【請求項１１】　上記送信情報の機密度に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしたことを特徴とする請求項７に記載の情報通信方法。

【請求項１２】　受信情報が暗号化されているか否かを判別し、上記受信情報が暗号化されていると判別された場合に、所定のエラー処理を行うようにしたことを特徴とする情報通信方法。

【請求項１３】　送信情報の暗号化手段および、情報の通信を行う際に上記暗号化手段の使用／不使用を選択する暗号処理選択手段を備えた情報送信装置と、

少なくとも暗号化されていない受信情報を解読する解読手段、受信情報が暗号化されているか否かを判別する暗号判別手段、および上記受信情報が暗号化されていると判別された場合に所定のエラー処理を行うエラー処理手段を備えた情報受信装置と、

から成ることを特徴とする情報通信システム。

【請求項１４】　送信情報の暗号化手段および、情報の通信を行う際に上記暗号化手段の使用／不使用を選択する暗号処理選択手段を備えた情報送信装置と、

受信情報が暗号化されているか否かを判別する暗号判別手段、および上記受信情報が暗号化されていると判別された場合に当該暗号化されている受信情報を解読する解読手段を備えた情報受信装置と、

から成ることを特徴とする情報通信システム。

【請求項１５】　上記暗号処理選択手段は、上記送信情報の暗号化処理を行うかどうかを指示するための指示手段を備え、情報送信者からの指示に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１３または１４に記載の情報通信システム。

【請求項１６】　上記暗号処理選択手段は、上記情報送信装置と上記情報受信装置とが接続されている通信媒体を判別する媒体判別手段を備え、接続されている通信媒体に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１３または１４に記載の情報通信システム。

【請求項１７】　上記暗号処理選択手段は、上記情報受信装置において暗号解読が可能であるかどうかを判別する暗号許可判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１３または１４に記載の情報通信システム。

【請求項１８】　上記暗号処理選択手段は、上記送信情報の機密度を判別する機密度判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択することを特徴とする請求項１３または１４に記載の情報通信システム。

【請求項１９】　請求項１～６の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２０】　請求項７～１２の何れか１項に記載の情報通信方法の処理手順をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報通信装置及び方法、情報通信システム、記録媒体に関するものである。

【０００２】

【従来の技術】

近年、携帯通信端末に代表される情報通信装置は、小型化、高機能化、情報処理の高速化が進み、携帯通信端末では既に、デスクトップ型のコンピュータに匹敵するほどの性能を持つものも発売されている。このことから、携帯通信端末は主にビジネスの分野において普及が急速に進んでおり、無線通信によって会社から離れた場合でも迅速に情報をやり取り出来るようになってきている。この場合に問題となるのが機密漏洩である。情報通信装置を開発するメーカーでは、それぞれの方法によって送信情報の暗号化処理技術の実用化を盛んに進めている。

【０００３】

また、現在では、通信機能としてデジタル映像を撮影して取り込み、その送信を行うことが可能となるなど、扱う情報量は急激に大きくなってきている。さらに、将来的には動画まで扱うことが考えられるので、情報信号処理部に求められる機能は更に高いものとなる。また、画像取り込み用のデジタルカメラを一体化した携帯通信端末が最近登場するようになり、将来的にはデジタルビデオカメラを含めた携帯通信端末が登場するのも近いと思われる。

【０００４】

しかし、携帯端末装置はこのような高機能化と引き換えに、通信機能や情報編集機能などのみを備えた以前の製品に比べると、携帯性を重視した小型化を達成することが益々困難な状況となってきている。こうした背景の中、更に暗号化処理を行うためには、情報処理スピードの向上はもちろんのこと、暗号処理装置を含めた情報通信装置全体の小型化が大きな課題となる。

【０００５】

【発明が解決しようとする課題】

上述したように、情報通信装置の中で現在問題とされているのは、高機能化に伴い価格が高くなってしまうこと、扱う情報が映像などを含めた膨大な量になりつつあること、さらに携帯端末などにおいては小型化が困難になってきたことである。

【０００６】

さらに、暗号化処理を行うことが可能な装置が最近注目を集めており、今後、暗号化処理手段を持つ通信装置が多く提供されることが予想される。一方、家庭

での使用を考えると、扱われる情報の機密度は比較的低く、必ずしも暗号化処理が必要であるとは言いきれない。しかし、暗号化処理された情報が常に送信されてくるとすれば、受信側も必ず暗号化された情報を解読する暗号解読装置を備えざるを得ない。結果として、送信側、受信側双方の装置の大型化、高価格化、情報処理に対する負担の増大は防げない。

【０００７】

本発明は、このような問題を解決するために成されたものであり、情報の暗号化処理を考慮しつつも通信携帯端末の小型化、低価格化、情報処理の負担減を実現できるようにすることを目的とする。

【０００８】

【課題を解決するための手段】

本発明の情報通信装置は、送信情報の暗号化手段と、情報の通信を行う際に、上記暗号化手段の使用／不使用を選択する暗号処理選択手段とを備えたことを特徴とする。

【０００９】

ここで、上記暗号処理選択手段は、上記送信情報の暗号化処理を行うかどうかを指示するための指示手段を備え、情報送信者からの指示に応じて上記暗号化手段の使用／不使用を選択するようにしても良い。

また、上記暗号処理選択手段は、情報送信側の装置と情報受信側の装置とが接続されている通信媒体を判別する媒体判別手段を備え、接続されている通信媒体に応じて上記暗号化手段の使用／不使用を選択するようにしても良い。

また、上記暗号処理選択手段は、情報受信側の装置において暗号解読が可能であるかどうかを判別する暗号許可判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択するようにしても良い。

また、上記暗号処理選択手段は、上記送信情報の機密度を判別する機密度判別手段を備え、その判別結果に応じて上記暗号化手段の使用／不使用を選択するようにしても良い。

【００１０】

本発明の他の態様では、受信情報が暗号化されているか否かを判別する暗号判

別手段と、上記暗号判別手段によって上記受信情報が暗号化されていると判別された場合に、所定のエラー処理を行うエラー処理手段とを備えたことを特徴とする。

【００１１】

また、本発明の情報通信方法は、情報の通信を行う際に、送信情報の暗号化処理の使用／不使用を選択するようにしたことを特徴とする。

【００１２】

ここで、情報送信者からの指示に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしても良い。

また、情報送信側の装置と情報受信側の装置とが通信可能な異なる通信媒体のうち、使用している通信媒体に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしても良い。

また、情報受信側の装置において暗号解読が可能であるかどうかの判別結果に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしても良い。

また、上記送信情報の機密度に応じて上記送信情報の暗号化処理の使用／不使用を選択するようにしても良い。

【００１３】

本発明の他の態様では、受信情報が暗号化されているか否かを判別し、上記受信情報が暗号化されていると判別された場合に、所定のエラー処理を行うようにしたことを特徴とする。

【００１４】

また、本発明の情報通信システムは、送信情報の暗号化手段および、情報の通信を行う際に上記暗号化手段の使用／不使用を選択する暗号処理選択手段を備えた情報送信装置と、少なくとも暗号化されていない受信情報を解読する解読手段、受信情報が暗号化されているか否かを判別する暗号判別手段、および上記受信情報が暗号化されていると判別された場合に所定のエラー処理を行うエラー処理手段を備えた情報受信装置と、から成ることを特徴とする。

本発明の他の態様では、送信情報の暗号化手段および、情報の通信を行う際に上記暗号化手段の使用／不使用を選択する暗号処理選択手段を備えた情報送信装

置と、受信情報が暗号化されているか否かを判別する暗号判別手段、および上記受信情報が暗号化されていると判別された場合に当該暗号化されている受信情報を解読する解読手段を備えた情報受信装置と、から成ることを特徴とする。

【００１５】

また、本発明のコンピュータ読み取り可能な記録媒体は、請求項１～６の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とする。

本発明の他の態様では、請求項７～１２の何れか１項に記載の情報通信方法の処理手順をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

【００１６】

【発明の実施の形態】

（第１の実施形態）

以下、本発明の一実施形態を図面に基づいて説明する。

ここで、本実施形態では、各機器間を接続するデジタルＩ／Ｆとして、無線の他にＩＥＥＥ１３９４シリアルバスを用いる場合についても考慮しているので、ＩＥＥＥ１３９４シリアルバスについてあらかじめ説明する。

【００１７】

《ＩＥＥＥ１３９４の技術の概要》

家庭用デジタルＶＴＲやＤＶＤの登場に伴なって、ビデオデータやオーディオデータなどのように、リアルタイムでかつ大情報量のデータ転送を行うためのサポートが必要になっている。こういったビデオデータやオーディオデータをリアルタイムで転送し、パソコン（ＰＣ）に取り込んだり、またはその他のデジタル機器に転送するには、必要な転送機能を備え高速にデータ転送可能なインタフェースが必要になってくる。そういった観点から開発されたインタフェースが、ＩＥＥＥ１３９４－１９９５（High Performance Serial Bus）（以下、１３９４シリアルバスと称する）である。

【００１８】

図４に、１３９４シリアルバスを用いて構成されるネットワーク・システムの

一例を示す。このシステムは複数の機器Ａ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆ，Ｇ，Ｈを備えており、Ａ－Ｂ間、Ａ－Ｃ間、Ｂ－Ｄ間、Ｄ－Ｅ間、Ｃ－Ｆ間、Ｃ－Ｇ間およびＣ－Ｈ間がそれぞれ１３９４シリアルバスのツイスト・ペア・ケーブルで接続されている。各機器間の接続方式は、ディジーチェーン方式とノード分岐方式とを混在可能としたものであり、自由度の高い接続が可能である。これらの機器Ａ～Ｈは、例としてＰＣ、デジタルＶＴＲ、ＤＶＤ、デジタルカメラ、ハードディスク、モニタ等である。

【００１９】

また、各機器は各固有のＩＤを有し、それぞれが互いのＩＤを認識し合うことによって、１３９４シリアルバスで接続された範囲において１つのネットワークを構成している。各デジタル機器間をそれぞれ１本の１３９４シリアルバスケーブルで順次接続するだけで、それぞれの機器が中継の役割を行い、全体として１つのネットワークを構成するものである。

【００２０】

また、１３９４シリアルバスの特徴でもあるＰｌｕｇ＆Ｐｌａｙ機能で、ケーブルを機器に接続した時点で機器の認識や接続状況などを自動的に認識する機能を有している。また、図４に示したようなシステムにおいて、ネットワークからある機器が削除されたり、または新たに追加されたときなどは、自動的にバスリセットを行い、それまでのネットワーク構成をリセットしてから、新たなネットワークの再構築を行う。この機能によって、その時々のネットワークの構成を常時設定、認識することができる。

【００２１】

また、データ転送速度は、１００／２００／４００Ｍｂｐｓと備えており、上位の転送速度を持つ機器が下位の転送速度をサポートし、互換をとるようになっている。データ転送モードとしては、コントロール信号などの非同期データ（Asynchronousデータ：以下、Async データと称する）を転送するAsynchronous転送モード、リアルタイムなビデオデータやオーディオデータ等の同期データ（Isochronous データ：以下、Iso データと称する）を転送するIsochronous 転送モードがある。このAsync データとIso データは、各サイクル（通常１サイクルは１

２５μＳ）の中において、サイクル開始を示すサイクル・スタート・パケット（ＣＳＰ）の転送に続き、Iso データの転送を優先しつつサイクル内で混在して転送される。

【００２２】

次に、図５に１３９４シリアルバスの構成要素を示す。

１３９４シリアルバスは、全体としてレイヤ（階層）構造で構成されている。図５に示したように、最もハード的なのが１３９４シリアルバスのケーブルであり、そのケーブルのコネクタが接続されるコネクタポートがあり、その上にハードウェアとしてフィジカル・レイヤとリンク・レイヤとがある。ハードウェア部は実質的なインタフェースチップの部分であり、そのうちフィジカル・レイヤは符号化やコネクタ関連の制御等を行い、リンク・レイヤはパケット転送やサイクルタイムの制御等を行う。

【００２３】

また、ファームウェア部のトランザクション・レイヤは、転送（トランザクション）すべきデータの管理を行い、ＲｅａｄやＷｒｉｔｅといった命令を出す。同じくファームウェア部のシリアルバスマネージメントは、接続されている各機器の接続状況やＩＤの管理を行い、ネットワークの構成を管理する部分である。このハードウェア部とファームウェア部までが、実質上の１３９４シリアルバスの構成である。

【００２４】

また、ソフトウェア部のアプリケーション・レイヤは、使うソフトによって異なる。これは、インタフェース上にどのようにデータをのせるかを規定する部分であり、ＡＶプロトコルなどのプロトコルによって規定されている。

以上が１３９４シリアルバスの構成である。

【００２５】

次に、図６に１３９４シリアルバスにおけるアドレス空間の図を示す。

１３９４シリアルバスに接続された各機器（ノード）には、必ず各ノード固有の６４ビットアドレスを持たせておく。そして、このアドレスをＲＯＭに格納しておくことで、自分や相手のノードアドレスを常時認識でき、相手を指定した通

信も行える。

【００２６】

１３９４シリアルバスのアドレッシングは、ＩＥＥＥ１２１２規格に準じた方式である。そのアドレス設定は、最初の１０ビットがバスの番号の指定用に、次の６ビットがノードＩＤ番号の指定用に使われる。残りの４８ビットが機器に与えられたアドレス幅になり、それぞれ固有のアドレス空間として使用できる。このうち最後の２８ビットは、固有データの領域として、各機器の識別や使用条件の指定の情報などを格納する。

【００２７】

以上が１３９４シリアルバスの技術の概要である。

次に、１３９４シリアルバスの特徴といえる技術の部分を、より詳細に説明する。

【００２８】

《１３９４シリアルバスの電気的仕様》

図７に、１３９４シリアルバスのケーブルの断面図を示す。１３９４シリアルバスでは、接続ケーブル内に、２組のツイストペア信号線の他に、電源ラインを設けている。これによって、電源を持たない機器や、故障により電圧低下した機器等にも電力の供給が可能になっている。電源線内を流れる電源の電圧は８～４０Ｖ、電流は最大電流ＤＣ１．５Ａと規定されている。

【００２９】

《ＤＳ－Ｌｉｎｋ符号化》

１３９４シリアルバスで採用されているデータ転送フォーマットのＤＳ－Ｌｉｎｋ符号化方式を説明するための図を、図８に示す。

１３９４シリアルバスでは、ＤＳ－Ｌｉｎｋ（Data/Strobe Link）符号化方式が採用されている。このＤＳ－Ｌｉｎｋ符号化方式は、高速なシリアルデータ通信に適しており、その構成は、２本の信号線を必要とする。２つのより対線のうち、一方に主となるデータを送り、他方のより対線にはストローブ信号を送る構成になっている。受信側では、通信されるデータとストローブ信号との排他的論理和をとることによって、クロックを再現できる。

【００３０】

このＤＳ－Ｌｉｎｋ符号化方式を用いるメリットとして、他のシリアルデータ転送方式に比べて転送効率が高いこと、ＰＬＬ回路が不要となるのでコントローラＬＳＩの回路規模を小さくできること、更には、転送すべきデータが無いときにアイドル状態であることを示す情報を送る必要が無いので、各機器のトランシーバ回路をスリープ状態にすることができ、これによって消費電力の低減が図れることなどが挙げられる。

【００３１】

《バスリセットのシーケンス》

１３９４シリアルバスでは、接続されている各機器（ノード）にはノードＩＤが与えられ、ネットワーク構成として認識されている。このネットワーク構成に変化があったとき、例えばノードの挿抜や電源のＯＮ／ＯＦＦなどによるノード数の増減などによって変化が生じて、新たなネットワーク構成を認識する必要があるときは、変化を検知した各ノードはバス上にバスリセット信号を送信して、新たなネットワーク構成を認識するモードに入る。なお、このときの変化の検知方法は、１３９４ポート基盤上でのバイアス電圧の変化を検知することによって行われる。

【００３２】

あるノードからバスリセット信号が伝達されると、各ノードのフィジカル・レイヤは、このバスリセット信号を受けると同時にリンク・レイヤにバスリセットの発生を伝達し、かつ、他のノードにバスリセット信号を伝達する。最終的にすべてのノードがバスリセット信号を検知した後、バスリセットが起動となる。

【００３３】

バスリセットは、先に述べたようなケーブル抜挿やネットワーク異常等のハード検出による起動の他に、プロトコルからのホスト制御などによってフィジカル・レイヤに直接命令を出すことによっても起動する。また、バスリセットが起動すると、データ転送は一時中断され、この間のデータ転送は待たされる。そして、バスリセットの終了後、新しいネットワーク構成のもとでデータ転送が再開される。以上がバスリセットのシーケンスである。

【００３４】

《ノードＩＤ決定のシーケンス》

バスリセットの後、各ノードは新しいネットワーク構成を構築するために、各ノードにＩＤを与える動作に入る。このときの、バスリセットからノードＩＤ決定までの一般的なシーケンスを図１６～図１８のフローチャートを用いて説明する。図１６のフローチャートには、バスリセットの発生からノードＩＤが決定され、データ転送が行えるようになるまでの一連のバスの作業を示してある。

【００３５】

図１６において、まず、ステップＳ１０１において、ネットワーク内にバスリセットが発生したかどうかを常時監視している。ここで、ノードの電源のＯＮ／ＯＦＦ等によってバスリセットが発生すると、ステップＳ１０２に移る。ステップＳ１０２では、ネットワークがリセットされた状態から、新たなネットワークの接続状況を知るために、直接接続されている各ノード間において親子関係の宣言がなされる。

【００３６】

次に、ステップＳ１０３において、全てのノード間で親子関係が決定すると、ステップＳ１０４で１つのルートノードが決定する。なお、すべてのノード間で親子関係を決定するまでは、ステップＳ１０２の親子関係の宣言を繰り返し行う。この間は、ルートノードも決定されない。ステップＳ１０４でルートノードが決定されると、次はステップＳ１０５において、各ノードにＩＤを与えるノードＩＤの設定作業が行われる。

【００３７】

このステップＳ１０５のＩＤ設定作業では、所定のノード順序でノードＩＤの設定が行われ、すべてのノードにＩＤが与えられるまで繰り返し行われる。最終的にステップＳ１０６ですべてのノードにＩＤを設定し終えたら、新しいネットワーク構成がすべてのノードにおいて認識されたので、各ノード間でデータ転送が行える状態となる。そして、ステップＳ１０７で実際にデータ転送が開始される。このステップＳ１０７の状態になると、ステップＳ１０１に戻って再びバスリセットが発生するのを監視するモードに入り、バスリセットが発生したらステ

ップＳ１０２からステップＳ１０６までの設定作業が繰り返し行われる。

【００３８】

以上が、図１６のフローチャートの説明であるが、図１６のフローチャートのバスリセットからルート決定までの部分と、ルート決定後からＩＤ設定終了までの部分の手順をより詳しく表したものが、それぞれ図１７、図１８である。

まず、図１７のフローチャートの説明を行う。

【００３９】

図１７において、ステップＳ２０１においてバスリセットが発生すると、ネットワーク構成は一旦リセットされる。なお、このステップＳ２０１では、バスリセットが発生するのを常に監視している。次に、ステップＳ２０２において、バスリセットされたネットワークの接続状況を再認識する作業の第１歩として、各機器（ノード）にリーフであることを示すフラグを立てておく。さらに、ステップＳ２０３において、各機器が自分の持つポートがいくつ他のノードと接続されているのかを調べる。

【００４０】

そして、ステップＳ２０４において、上記ステップＳ２０３におけるポート数の確認結果に応じて、これから親子関係の宣言を始めていくために、未定義（親子関係が決定されてない）ポートの数を調べる。バスリセットの直後はポート数＝未定義ポート数であるが、親子関係が決定されていくに従って、ステップＳ２０４で検知する未定義ポートの数は変化していくものである。

【００４１】

まず、バスリセットの直後、はじめに親子関係の宣言を行えるのはリーフに限られている。リーフとは、未定義ポート数が１つだけのノードのことであり、これはステップＳ２０３のポート数の確認で知ることができる。上記ステップＳ２０４でリーフであると認識されたノードは、ステップＳ２０５において、自分に接続されているノードに対して「自分は子、相手は親」と宣言し、動作を終了する。

【００４２】

一方、ステップＳ２０３でポート数が複数あり、ブランチであると認識された

ノードについては、バスリセットの直後はステップＳ２０４で「未定義ポート数＞1」と判断されるので、ステップＳ２０６へと移り、まずブランチというフラグが立てられる。そして、ステップＳ２０７でリーフからの親子関係宣言で「親」の受付をするために待つ。

【００４３】

リーフが親子関係の宣言を行い、ステップＳ２０７でこの宣言を受けたブランチは、適宜ステップＳ２０４の未定義ポート数の確認を行う。ここで、未定義ポート数が１になっていれば、残っているポートに接続されているノードに対して、ステップＳ２０５において「自分が子」の宣言をすることが可能になる。２度目以降、ステップＳ２０４で未定義ポート数を確認しても２つ以上あるブランチに対しては、再度ステップＳ２０７でリーフまたは他のブランチから「親」の受付をするために待つ。

【００４４】

最終的に、いずれか１つのブランチ、または例外的にリーフ（子宣言を行えるのにすばやく動作しなかったため）がステップＳ２０４の未定義ポート数の確認結果としてゼロになったら、これにてネットワーク全体の親子関係の宣言が終了したものとなる。このとき、未定義ポート数がゼロ（すべて親のポートとして決定）になった唯一のノードは、ステップＳ２０８でルートのフラグが立てられ、ステップＳ２０９でルートとしての認識がなされる。

このようにして、図１７に示したバスリセットからネットワーク内すべてのノード間における親子関係の宣言までの処理が終了する。

【００４５】

次に、図１８のフローチャートについて説明する。

まず、図１７までのシーケンスで各ノードに対してリーフ、ブランチ、ルートというフラグの情報が設定されているので、これをもとにして、ステップＳ３０１でそれぞれのノードを分類する。各ノードにＩＤを与える作業として、最初にＩＤの設定を行うことができるのはリーフからである。すなわち、リーフ→ブランチ→ルートの順で若い番号（ノード番号＝０～）からＩＤの設定がなされていく。

【００４６】

ステップＳ３０２において、ネットワーク内に存在するリーフの数Ｎ（Ｎは自然数）を設定する。この後、ステップＳ３０３において、各リーフがルートに対してＩＤを与えるように要求する。この要求が複数ある場合には、ルートはステップＳ３０４でアービトレーション（１つに調停する作業）を行い、テップＳ３０５で、この調停に勝ったノード１つにＩＤ番号を与えるとともに、負けたノードには失敗の結果通知を行う。

【００４７】

次に、ステップＳ３０６において、リーフがＩＤを取得できたかどうかを確認し、ＩＤ取得が失敗に終わった場合は、当該リーフは、ステップＳ３０３に戻って再度ＩＤ要求を出し、同様の作業を繰り返す。ＩＤを取得できた場合には、ステップＳ３０７において、当該リーフからそのノードのＩＤ情報をブロードキャストで全ノードに転送する。

【００４８】

１つのリーフについてノードＩＤ情報のブロードキャストが終わると、ステップＳ３０８で残りのリーフの数が１つ減らされる。そして、ステップＳ３０９において、この残りのリーフ数が１つ以上あるかどうかを確認し、１つ以上あるときは、次のリーフについてステップＳ３０３のＩＤ要求の作業から同様の処理を繰り返し行う。

【００４９】

最終的にすべてのリーフがＩＤ情報をブロードキャストすると、ステップＳ３０９の判断結果がＮ＝０となり、次はブランチのＩＤ設定に移る。ブランチのＩＤ設定もリーフの時と同様に行われる。すなわち、まず、ステップＳ３１０においてネットワーク内に存在するブランチの数Ｍ（Ｍは自然数）を設定する。この後、ステップＳ３１１において、各ブランチがルートに対してＩＤを与えるように要求する。

【００５０】

これに対してルートは、ステップＳ３１２でアービトレーションを行い、ステップＳ３１３で、この調停に勝ったブランチから順に、リーフに与え終った次の

若い番号からＩＤを与えていく。また、このステップＳ３１３において、ルートは、ＩＤ要求を出したブランチに対してＩＤ情報または失敗結果を通知する。次に、ステップＳ３１４では、ブランチがＩＤを取得できたかどうかを確認し、ＩＤ取得が失敗に終わった場合は、当該ブランチは、ステップＳ３１１に戻って再度ＩＤ要求を出し、同様の作業を繰り返す。ＩＤを取得できた場合には、ステップＳ３１５において、当該ブランチからそのノードのＩＤ情報をブロードキャストで全ノードに転送する。

【００５１】

１つのノードＩＤ情報のブロードキャストが終わると、ステップＳ３１６で残りのブランチの数が１つ減らされる。そして、ステップＳ３１７において、この残りのブランチの数が１つ以上あるかどうかを確認し、１つ以上あるときは、次のブランチについてステップＳ３１１のＩＤ要求の作業から同様の処理を繰り返し行う。これは、最終的にすべてのブランチがＩＤ情報をブロードキャストするまで行われる。すべてのブランチがノードＩＤを取得すると、ステップＳ３１７の判断結果はＭ＝０となり、ブランチのＩＤ取得モードも終了する。

【００５２】

ここまで終了すると、最終的にＩＤ情報を取得していないノードはルートのみとなる。ルートは、ステップＳ３１８において、今までにリーフやブランチに与えていない番号で最も大きい番号を自分のＩＤ番号として設定し、ステップＳ３１９でそのルートのＩＤ情報を全てのノードにブロードキャストする。

以上で、図１８に示したように、親子関係が決定した後から、すべてのノードのＩＤが設定されるまでの手順が終了する。

【００５３】

次に、一例として図９に示した実際のネットワークにおける動作を、図９を参照しながら説明する。図９の例では、（ルート）ノードＢの下位にはノードＡとノードＣが直接接続されており、更にノードＣの下位にはノードＤが直接接続されており、更にノードＤの下位にはノードＥとノードＦが直接接続された階層構造になっている。この階層構造やルートノード、ノードＩＤを決定する手順を以下に説明する。

【００５４】

バスリセットがされた後、まず各ノードの接続状況を認識するために、各ノードの直接接続されているポート間において、親子関係の宣言がなされる。この親子とは、親側が階層構造で上位となり、子側が下位となるということである。図９の例では、バスリセットの後、最初に親子関係の宣言を行ったのはノードＡである。

【００５５】

すなわち、基本的には、ノードの１つのポートにのみ接続があるノード（リーフ）から親子関係の宣言を行うことができる。これは、各ノードは自分には１つのポートの接続があるのみということをまず知ることができるので、これによってネットワークの端であることを認識し、親子関係の宣言を行う。その中で早く動作を行ったノードから親子関係が決定されていく。このとき、親子関係の宣言を行った側（Ａ－Ｂ間ではノードＡ）のポートが子と設定され、相手側（Ａ－Ｂ間ではノードＢ）のポートが親と設定される。こうして、ノードＡ－Ｂ間で子－親、ノードＥ－Ｄ間で子－親、ノードＦ－Ｄ間で子－親と決定される。

【００５６】

さらに１階層上がって、今度は複数個の接続ポートを持つノード（ブランチ）のうち、他ノードからの親子関係の宣言を受けたものから順次、更に上位に親子関係の宣言を行っていく。図９の例では、まずノードＤがＤ－Ｅ間、Ｄ－Ｆ間と親子関係が決定した後、ノードＣに対する親子関係の宣言を行っており、その結果ノードＤ－Ｃ間で子－親と決定している。ノードＤからの親子関係の宣言を受けたノードＣは、もう一つのポートに接続されているノードＢに対して親子関係の宣言を行っている。これによってノードＣ－Ｂ間で子－親と決定している。

【００５７】

このようにして、図９のような階層構造が構成され、最終的に接続されているすべてのポートにおいて親となったノードＢが、ルートノードと決定された。ルートは１つのネットワーク構成中に１つしか存在しないものである。

なお、この図９においてはノードＢがルートノードと決定されているが、ノードＡから親子関係の宣言を受けたノードＢが、他のノードに対して親子関係の宣

言を早いタイミングで行っていれば、ルートノードは他ノードに移っていたこともあり得る。すなわち、伝達されるタイミングによってはどのノードもルートノードとなる可能性があり、同じネットワーク構成でもルートノードは一定とは限らない。

【００５８】

ルートノードが決定すると、次は各ノードＩＤを決定するモードに入る。ここではすべてのノードが、決定した自分のノードＩＤを他のすべてのノードに通知する（ブロードキャスト機能）。自己ＩＤ情報は、自分のノード番号、接続されている位置の情報、持っているポートの数、接続のあるポートの数、各ポートの親子関係の情報等を含んでいる。

【００５９】

ノードＩＤ番号の割り振りの手順としては、まず１つのポートにのみ接続があるノード（リーフ）から起動することができ、この中から順にノード番号＝０、１、２、……と割り当てられる。ノードＩＤを手にしたノードは、ノード番号を含む情報をブロードキャストで各ノードに送信する。これによって、そのＩＤ番号は『割り当て済み』であることが認識される。

【００６０】

すべてのリーフが自己ノードＩＤを取得し終ると、次はブランチへと処理が移り、リーフに引き続いたノードＩＤ番号が各ノードに割り当てられる。リーフと同様に、ノードＩＤ番号が割り当てられたブランチから順次ノードＩＤ情報をブロードキャストし、最後にルートノードが自己ＩＤ情報をブロードキャストする。すなわち、常にルートは最大のノードＩＤ番号を所有するものである。

以上のようにして、階層構造全体のノードＩＤの割り当てが終わり、ネットワーク構成が再構築され、バスの初期化作業が完了する。

【００６１】

《アービトレーション》

１３９４シリアルバスでは、データ転送に先立って必ずバス使用権のアービトレーション（調停）を行う。１３９４シリアルバスは、個別に接続された各機器が転送された信号をそれぞれ中継することによって、ネットワーク内すべての機

器に同信号を伝えるように構成された、論理的なバス型ネットワークである。よって、パケットの衝突を防ぐ意味でアービトレーションは必要である。これにより、ある時間にはたった１つのノードのみがデータ転送を行うことができる。

【００６２】

アービトレーションを説明するための図として、図１０（ａ）にバス使用権要求の図を示し、図１０（ｂ）にバス使用権許可の図を示す。以下、この図１０を用いてバスアービトレーションについて説明する。

アービトレーションが始まると、１つもしくは複数のノードが親ノードに向かって、それぞれバス使用権の要求を発する。図１０（ａ）のノードＣとノードＦがバス使用権の要求を発しているノードである。これを受けた親ノード（図１０ではノードＡ）は、更にその親ノードに向かって、バス使用権の要求を発する（中継する）。この要求は、最終的に調停を行うルートに届けられる。

【００６３】

バス使用権の要求を受けたルートノードは、どのノードにバスを使用させるかを決める。この調停作業はルートノードのみが行えるものであり、調停によって勝ったノードには、バスの使用許可を与える。図１０（ｂ）の例では、ノードＣに使用許可が与えられ、ノードＦの使用は拒否されたことが示されている。一方、アービトレーションに負けたノードに対しては、ＤＰ（data prefix ）パケットを送り、拒否されたことを知らせる。拒否されたノードのバス使用要求は、次回のアービトレーションまで待たされる。

以上のようにして、アービトレーションに勝ってバスの使用許可を得たノードは、以降データの転送を開始できる。

【００６４】

ここで、アービトレーションの一連の流れを図１９のフローチャートに示す。以下、このフローチャートに従って説明する。

ノードがデータ転送を開始できるためには、バスがアイドル状態であることが必要である。先に行われていたデータ転送が終了して、現在バスが空き状態であることを認識するためには、各転送モードで個別に設定されている所定のアイドル時間ギャップ長（例えば、サブアクション・ギャップ）を経過したかどうかで

判断する。このギャップ長を経過することによって、各ノードは自分のデータ転送が開始できると判断する。

【００６５】

すなわち、まずステップＳ４０１において、Async データ、Iso データ等のそれぞれ転送するデータに応じた所定のギャップ長が得られたかどうかを判断する。所定のギャップ長が得られない限り、データ転送を開始するために必要なバス使用権の要求はできないので、所定のギャップ長が得られるまで待つ。ステップＳ４０１で所定のギャップ長が得られたら、ステップＳ４０２に進んで転送すべきデータがあるかどうかを判断する。

【００６６】

転送すべきデータがある場合は、ステップＳ４０３において、データ転送を行うためにバスを確保するよう、バス使用権の要求をルートに対して発する。このときのバス使用権の要求を表す信号は、図１０に示したように、ネットワーク内各機器を中継しながら、最終的にルートに届けられる。一方、上記ステップＳ４０２で転送するデータがないと判断した場合は、そのまま待機する。

【００６７】

次に、ステップＳ４０４において、ステップＳ４０３において発行されたバス使用要求を少なくとも１つ以上ルートが受信したら、ルートはステップＳ４０５において、使用要求を出したノードの数を調べる。ステップＳ４０５で調べた結果、バス使用要求を出したノードが１つだったら、そのノードに直後のバス使用許可が与えられることとなる。

【００６８】

一方、上記ステップＳ４０５で、使用要求を出したノードが複数であると判断した場合は、ルートは、ステップＳ４０６において、使用許可を与えるノードを１つに決定する調停作業を行う。この調停作業は公平なものであり、毎回同じノードばかりが許可を得るようなことはなく、平等に権利を与えていくような構成となっている。そして、ステップＳ４０７において、使用要求を出した複数ノードの中からルートが調停して使用許可を得た１つのノードと、調停に敗れたその他のノードとに分ける選択を行う。

【００６９】

ここで、ルートは、ステップＳ４０６でルートにより調停されて使用許可を得た１つのノード、またはステップＳ４０５での選択値から「使用要求ノード数＝１」として調停無しに使用許可を得たノードに対しては、ステップＳ４０８において許可信号を送る。許可信号を得たノードは、受け取った直後に転送すべきデータ（パケット）の転送を開始する。

【００７０】

また、ステップＳ４０６の調停で敗れて、バス使用が許可されなかったノードに対しては、ステップＳ４０９においてルートからアービトレーション失敗を示すＤＰ（data prefix ）パケットが送られる。これを受け取ったノードは、データ転送を行うためのバス使用要求を再度出すため、ステップＳ４０１まで戻り、所定ギャップ長が得られるまで待機する。

以上が、アービトレーションの流れを説明した図１９のフローチャートの説明である。

【００７１】

《Asynchronous（非同期）転送》

アシンクロナス転送は、非同期転送である。図１１に、アシンクロナス転送における時間的な遷移状態を示す。図１１に示されている最初のサブアクション・ギャップは、バスのアイドル状態を示すものである。このアイドル時間が一定値になった時点で、データ転送を希望するノードはバスが使用できると判断して、バス獲得のためのアービトレーションを実行する。

【００７２】

アービトレーションでバスの使用許可を得ると、次にデータの転送がパケット転送の形式で実行される。データ転送後、このデータを受信したノードは、転送されたデータに対する受信結果としてのａｃｋ（受信確認用返送コード）を、ack gap という短いギャップの後、返送して応答するか、応答パケットを送ることによって転送が完了する。受信確認用返送コードａｃｋは、４ビットの情報と４ビットのチェックサムとからなり、データ転送成功か、ビジー状態か、ペンディング状態であるかといった情報を含み、すぐに送信元ノードに返送される。

【００７３】

次に、図１２にアシンクロナス転送のパケットフォーマットの例を示す。パケットには、データ部および誤り訂正用のデータＣＲＣの他にはヘッダ部がある。このヘッダ部には、図１２に示したような目的ノードＩＤ、ソースノードＩＤ、転送データ長さや各種コードなどが書き込まれ、転送が行われる。

また、アシンクロナス転送は、自己ノードから相手ノードへの１対１の通信である。転送元ノードから転送されたパケットは、ネットワーク中の各ノードに行き渡るが、自分宛てのアドレス以外のものは無視されるので、宛先の１つのノードのみが読み込むことになる。

以上がアシンクロナス転送の説明である。

【００７４】

《Isochronous （同期）転送》

アイソクロナス転送は同期転送である。１３９４シリアルバスの最大の特徴であるとも言えるこのアイソクロナス転送は、特にＶＩＤＥＯ映像データや音声データといったマルチメディアデータなど、リアルタイムな転送を必要とするデータの転送に適した転送モードである。また、アシンクロナス（非同期）転送が１対１の転送であったのに対し、このアイソクロナス転送は、ブロードキャスト機能によって、転送元の１つのノードから他のすべてのノードへ一様にデータが転送される。

【００７５】

図１３は、アイソクロナス転送における時間的な遷移状態を示す図である。アイソクロナス転送は、バス上の一定時間毎に実行される。この時間間隔をアイソクロナスサイクルと呼ぶ。アイソクロナスサイクル時間は、１２５μＳである。この各サイクルの開始時間を示し、各ノードの時間調整を行う役割を担っているのがサイクル・スタート・パケットである。

【００７６】

サイクル・スタート・パケットを送信するのは、サイクル・マスタと呼ばれるノードである。サイクル・マスタは、１つ前のサイクル内のデータ転送終了後、所定のアイドル期間（サブアクションギャップ）を経た後、本サイクルの開始を

告げるサイクル・スタート・パケットを送信する。このサイクル・スタート・パケットの送信される時間間隔が１２５μＳとなる。

【００７７】

また、図１３にチャネルＡ、チャネルＢ、チャネルＣと示したように、１サイクル内において複数種のパケットがチャネルＩＤをそれぞれ与えられることによって、複数のパケットを１サイクル内で区別して転送できる。これによって、同時に複数ノード間でのリアルタイムな転送が可能である。また、受信するノードでは、複数のパケットのうち、自分が欲しいチャネルＩＤのデータのみを取り込む。このチャネルＩＤは、送信先のアドレスを表すものではなく、データに対する論理的な番号を与えているに過ぎない。よって、あるパケットは、１つの送信元ノードから他のすべてのノードに行き渡るブロードキャストで転送されることになる。

【００７８】

アイソクロナス転送のパケット送信に先立って、アシンクロナス転送と同様にバス使用権のアービトレーションが行われる。しかし、アイソクロナス転送は、アシンクロナス転送のように１対１の通信ではないので、アイソクロナス転送にはａｃｋ（受信確認用返信コード）は存在しない。

【００７９】

また、図１３に示したiso gap （アイソクロナスギャップ）とは、アイソクロナス転送を行う前にバスが空き状態であると認識するために必要なアイドル期間を表している。この所定のアイドル期間を経過すると、アイソクロナス転送を行いたいノードはバスが空いていると判断し、転送前のアービトレーションを行うことができる。

【００８０】

次に、図１４にアイソクロナス転送のパケットフォーマットの例を示し、これについて説明する。

各チャネルに分かれた各種のパケットには、それぞれデータ部および誤り訂正用のデータＣＲＣの他にヘッダ部がある。このヘッダ部には、図１４に示したような転送データ長やチャネルＮＯ、その他各種コードおよび誤り訂正用のヘッダ

ＣＲＣなどが書き込まれ、転送が行われる。

以上がアイソクロナス転送の説明である。

【００８１】

《バス・サイクル》

実際の１３９４シリアルバス上の転送では、アイソクロナス転送とアシンクロナス転送とは混在できる。そのときの、アイソクロナス転送とアシンクロナス転送とが混在した、バス上の転送状態の時間的な遷移の様子を、図１５に示す。

【００８２】

アイソクロナス転送は、アシンクロナス転送より優先して実行される。その理由は、サイクル・スタート・パケットの後、アシンクロナス転送を起動するために必要なアイドル期間のギャップ長（サブアクションギャップ）よりも短いギャップ長（アイソクロナスギャップ）で、アイソクロナス転送を起動できるからである。したがって、アイソクロナス転送は、アシンクロナス転送より優先して実行されることとなる。

【００８３】

図１５に示した一般的なバスサイクルにおいて、サイクル＃ｍのスタート時にサイクル・スタート・パケットがサイクル・マスタから各ノードに転送される。これによって、各ノードで時刻調整が行われる。アイソクロナス転送を行うべきノードは、所定のアイドル期間（アイソクロナスギャップ）を待ってからアービトレーションを行い、パケット転送に入る。図１５ではチャネルｅ、チャネルｓ、チャネルｋのパケットがこの順にアイソクロナス転送されている。

【００８４】

このアービトレーションからパケット転送までの動作を与えられているチャネル分だけ繰り返し行った後、サイクル＃ｍにおけるアイソクロナス転送がすべて終了したら、次にアシンクロナス転送を行うことができるようになる。すなわち、アイソクロナス転送終了後のアイドル時間が、アシンクロナス転送を行うことが可能なサブアクションギャップに達することにより、アシンクロナス転送を行いたいノードは、アービトレーションの実行に移れると判断する。ただし、アシンクロナス転送が行えるのは、アイソクロナス転送終了後から次のサイクル・ス

タート・パケットを転送すべき時間（cycle synch ）までの間にアシンクロナス転送を起動するためのサブアクションギャップが得られた場合に限っている。

【００８５】

図１５のサイクル＃ｍでは、３つのチャネル分のアイソクロナスパケットがアイソクロナス転送された後、アシンクロナスパケット（含むａｃｋ）が２パケット分だけ（パケット１、パケット２）転送されている。このアシンクロナスパケット２の後は、サブアクションギャップに達する前に次のサイクル＃ｍ＋１をスタートすべき時間（cycle synch ）に至るので、サイクル＃ｍでのデータ転送はここまでで終わる。

【００８６】

ただし、非同期または同期転送動作中に次のサイクル・スタート・パケットを送信すべき時間（cycle synch ）に至ったとしたら、データ転送を無理に中断せず、その転送が終了した後のアイドル期間を待ってから次サイクルのサイクル・スタート・パケットを送信する。すなわち、１つのサイクルが１２５μＳ以上続いたときは、その分次サイクルは基準の１２５μＳより短縮されたとする。このように、アイソクロナスサイクルは、１２５μＳを基準としてそれよりも超過、短縮し得るものである。

【００８７】

なお、アイソクロナス転送は、リアルタイム転送を維持するために毎サイクル必要であれば必ず実行され、アシンクロナス転送は、サイクル時間が短縮されたことによって次以降のサイクルにまわされることもある。こういった遅延情報も含めて、サイクル・マスタによって管理される。

以上が、ＩＥＥＥ１３９４シリアルバスの説明である。

【００８８】

次に、本実施形態における暗号化の方法について簡単に述べる。

一般的な通信情報の暗号化の方式としては、共通鍵暗号と公開鍵暗号の２つの方式が主に用いられている。まず、前者の共通鍵暗号方式について説明する。

【００８９】

《共通鍵暗号方式》

暗号アルゴリズムのうち、暗号化および復号化において共通の鍵を用いるのが共通鍵暗号と呼ばれる方式である。この方式は、ストリーム型暗号、ブロック型暗号の２つの方式に大別される。

【００９０】

（１）ストリーム型暗号

ストリーム型暗号は、例えば“０”と“１”のビットによる平文を暗号化する場合に、その１ビットごとに、乱数よって発生させた“１”か“０”による１ビットの鍵を排他的論理和によって加えていくことによって、暗号化を行う。暗号化された情報は、１ビットずつ順次送信可能であるため、情報送信スピードの高速化が可能であるという利点がある。さらに、１ビットごとの暗号化であるために、暗号化エラーが他のビットに波及しないなどの利点もある。しかし、送信側と受信側とで送信文と同じ情報量の乱数による鍵を共有化することは困難であるために、あらかじめ共有し合った短い乱数をもとに、比較的簡単な関数を用いて疑似乱数を生成し、これを用いるのが主流である。

【００９１】

（２）ブロック型暗号

ブロック型暗号は、平文を何ビットか入力して１ブロックの集合になったら、ブロック全体を暗号変換して１ブロックの暗号文として出力する方式である。このブロック型暗号では、平文の換字、転置などの比較的簡単な計算によって暗号を構成できる。すなわち、この方式では、１ブロックの平文に対して鍵という数値パラメータによって換字、転置を行う。次に、送信されてきた情報も１ブロックごとに同様に暗号化を行う。

【００９２】

この方法では、上記ストリーム型暗号のような１ビットごとの暗号化とは異なり、単純に換字、転置を繰り返すのみであるために、暗号化情報を均一にランダム化させるのが困難であるという欠点がある。さらに、均一ランダム化に近づけるためには、換字、転置を多数回繰り返す必要があるために、転送時間が長くなるという欠点もある。

【００９３】

《公開鍵暗号方式》

暗号アルゴリズムの中で、暗号化に用いる鍵と復号化に用いる鍵とが異なるものを公開鍵暗号方式と呼ぶ。この方式では、暗号化のための鍵を情報通信を行う相手に公開するとともに、その鍵を用いて暗号化された情報を復号するための鍵を、秘密に保持する。公開された鍵を公開鍵と呼び、秘密に保持された鍵を秘密鍵と呼ぶ。公開鍵から秘密鍵を予測することは不可能であるが、この２つの鍵は１対となっており、公開鍵による暗号情報は秘密鍵でのみ復号化される。

【００９４】

この方式では、鍵の保守性が高くなる（秘密鍵のみ自分で保持すればよい）という利点があるが、共通鍵暗号方式に比べて処理に千倍近い時間がかかるという欠点がある。そこで、最近では、共通鍵暗号と公開鍵暗号とを両立させた方式が用いられるようになってきている。以下にその例を説明する。

【００９５】

送信者はまず、受信者に公開鍵の送信を要求し、受信者からの公開鍵暗号によって暗号化された共通鍵を受信者に送信し、両者の間で共通鍵暗号の共有がなされる。ここで、共通鍵暗号による暗号化を行った情報を送信すれば、処理時間が比較的短くて済むことになる。

本実施形態では、暗号化方式として、上記に説明した各方式のいずれかを用いるものとする。

【００９６】

図１は、本発明の一実施形態による携帯通信端末の概略構成図であり、（ａ）は送信側ＰＤＡ（Personal Digital Assistants ）装置の構成を示し、（ｂ）は受信側ＰＤＡ装置の構成を示している。

【００９７】

図１（ａ）に示されるように、本実施形態の送信側ＰＤＡ装置１は、端末内で様々な機能を実行する情報処理部３と、暗号処理選択部４と、暗号化信号処理部５と、実際に情報の送受信を行う情報送受信部６とから構成されている。暗号処理選択部４は、送信側ＰＤＡ装置１と受信側ＰＤＡ装置２とが図示しないサーバに１３９４シリアルバスなどで直接接続されているか、あるいは受信側ＰＤＡ装

置２に暗号処理部が具備されているかどうか、あるいは送信者から暗号化請求があったどうかを識別し、その結果に応じて暗号化処理を行うかどうかを選択する。また、暗号化信号処理部５は、信号の暗号化と、暗号化された信号を元の信号に変換する処理とを行う。

【００９８】

また、図１（ｂ）に示されるように、受信側ＰＤＡ装置２は、送信側ＰＤＡ装置１内の情報処理部３および情報送受信部６と同様の情報処理部７および情報送受信部９と、暗号化された情報信号を受信してしまった場合に、送信者と受信者とに受信エラーを知らせる受信エラー処理部８と、受信エラー表示部１０とから構成されている。本実施形態において受信側の携帯通信端末２は、送信側の暗号化信号処理部５に相当する構成は備えておらず、暗号化された信号を受信してもそれを復号化して利用することができないものである。

【００９９】

以下に、上記のように構成された携帯通信端末間での通信の動作を説明する。まず、送信側ＰＤＡ装置１の情報処理部３によって生成された情報信号ｄ１は、暗号化信号処理部５に送られる。ここで、暗号処理選択部４によって、暗号化を行う請求信号ｄ３が出力されている場合には、上記生成された情報信号ｄ１は暗号化信号ｄ２に変換されて情報送受信部６に送られ、送信が開始される。一方、暗号化請求信号ｄ３がなかった場合には、情報信号ｄ１はそのまま情報送受信部６に送られ、送信される。

【０１００】

受信側ＰＤＡ装置２は、情報送受信部９によって情報信号ｄ１か暗号化信号ｄ２を受信する。この受信した信号は、暗号化されたものかそうでないかを判別するために、受信エラー処理部８に送られる。そして、受信エラー処理部８において、上記受信した信号が暗号化されたものか否かを判別した結果、暗号化された信号ｄ２だった場合には、受信エラー表示部１０を用いて受信者にその旨を表示するとともに、更に送信元にも受信エラーのメッセージｄ４を送信する。一方、暗号化されていない情報信号ｄ１を受信したと判別された場合には、その情報信号ｄ１は情報処理部７に送られ、利用される。

【０１０１】

次に、図２のフローチャートに、本実施形態による携帯通信端末の動作手順を示す。なお、図２（ａ）は送信側のフローチャートを示し、図２（ｂ）は受信側のフローチャートを示している。

図２（ａ）において、まず、ステップＳ１で送信側から情報の通信要求があった場合、ステップＳ２において、暗号処理選択部４によって送信者による暗号化処理要求があったかどうかを判別する。

【０１０２】

ここでいう暗号化処理要求は、

１．送信者によって予め設定された情報の機密度が高い場合

２．送信者によって予め設定された受信者に情報の送信を行う場合

３．送信者によって暗号化請求が予め設定されている場合

などに行われ、暗号化要求信号ｄ５が発生する。暗号化要求信号ｄ５があった場合は、暗号処理選択部４は暗号化信号処理部５に対して暗号化請求信号ｄ３を発行する。これに応じて暗号化信号処理部５は、ステップＳ５で情報の暗号化処理を実行する。

【０１０３】

一方、上記ステップＳ２で暗号化要求信号ｄ５がなかったと判断された場合には、ステップＳ３に進み、送信側ＰＤＡ装置１と受信側ＰＤＡ装置２とが、当該送信端末と受信端末とが登録されている図示しないサーバに直接接続されているかどうかが判別される。これは、図１に示されるように、図示しないサーバから送られてくる携帯通信端末の接続状況信号ｄ８を暗号処理選択部４が受け取り、これに基づいて判別する。

【０１０４】

ここで、どちらともサーバに直接接続されている場合は、暗号処理選択部４は暗号化信号処理部５に対して暗号化請求信号ｄ３を発行する。これに応じて暗号化信号処理部５は、ステップＳ５で情報の暗号化処理を実行する。一方、少なくとも何れかがサーバに直接接続されていない場合は、更にステップＳ４に進み、受信側ＰＤＡ装置２が暗号化を許可しているかどうかを判別する。

【０１０５】

このステップＳ４における判別方法としては、受信側ＰＤＡ装置２を暗号化の可／不可も併せてサーバなどに予め登録しておき、これを参照することによって判別する形態がある。また、他の方法としては、図１に示されるように、先に送信側の暗号処理選択部４から受信側の情報処理部７に判別要求信号ｄ６を送信して、受信側の情報処理部７にて暗号化の可／不可を判別する。そして、その暗号化の可／不可を表す判別信号ｄ７（図１の例では「不可」の信号）を受信側の情報処理部７から送信側の暗号処理選択部４に返信させる形態も考えられる。

【０１０６】

ここで、暗号化が不可であるという判別結果を得た場合には、ステップＳ５の暗号化処理を行うことなくステップＳ６で情報信号の送信を開始する。また、暗号化信号が可であるという判別結果を得た場合は、暗号処理選択部４は暗号化信号処理部５に対して暗号化請求信号ｄ３を発行する。これに応じて暗号化信号処理部５は、ステップＳ５で暗号化処理を行い、その後、ステップＳ６で上記暗号化した信号を送信する。

【０１０７】

受信側ＰＤＡ装置２は、ステップＳ７で信号を受信すると、まず、ステップＳ８で上記受信した信号を図示しないサブメモリに格納し、ステップＳ９でこの受信信号が暗号化されているかどうかを受信エラー処理部８によって判別する。受信した信号が暗号化された信号であった場合は、まずステップＳ１１で受信エラー表示部１０を用いて受信者に受信エラーを表示し、さらにステップＳ１２で、送信元に対して受信エラーのメッセージｄ４を送信する。

【０１０８】

また、受信した信号が暗号化されていない信号であった場合は、ステップＳ１０でその受信信号をそのまま図示しないメインメモリに格納し、ステップＳ１３で受信処理を終了する。このメインメモリに格納された情報信号ｄ１は、その後情報処理部７にて利用することが可能である。

【０１０９】

図３は、受信側ＰＤＡ装置２が図１（ａ）の送信側ＰＤＡ装置１と同じ形態の

ものであった場合の処理を示すフローチャートである。

まず、ステップＳ１７で信号を受信すると、ステップＳ１８で上記受信した信号を図示しないサブメモリに格納し、ステップＳ１９でこの受信信号が暗号化された信号かどうかを判別する。

【０１１０】

ここで、受信した信号が暗号化された信号であった場合は、ステップＳ２０に進み、暗号化信号処理部５によって暗号が解読される。そして、ステップＳ２１でその解読された信号が図示しないメインメモリに格納され、ステップＳ２２で受信処理を終了する。一方、受信した信号が暗号化されていなかった場合には、ステップＳ２１でその信号がそのまま図示しないメインメモリに格納されて、ステップＳ２２で受信処理を終了する。

【０１１１】

以上のように、本実施形態によれば、情報送信側が情報の暗号化を行うか否かを選択できる暗号処理選択部４を備えることによって、暗号化処理をなるべく省略し、信号処理の負担や、暗号化に伴う処理の負担を軽減することができる。また、情報受信側が暗号化に関する機能を備えていない場合に、暗号化された信号を受信側に送ってしまっても、受信側ではそれを受信エラーとして対応し、送信者および受信者の両方にエラー表示することができるので、通信の不備をいち早く発見して適切な対応をとることができる。

【０１１２】

この場合、暗号処理選択部４では、例えば、送信する情報の機密度を判別し、その機密度に応じて暗号化処理の使用／不使用を決定する。例えば、１つの情報通信端末を家庭用、ビジネス用の両方に用いる場合が考えられる。この場合、家族との情報通信においては暗号化処理を行わず、会社との情報通信においては暗号化処理を行って機密を保持する使用法が考えられる。このとき、情報送信者が所定の受信者のアドレスを自己の情報通信端末に予め登録しておき、この登録されたアドレスとの通信においては暗号化処理を自動的に行わないようにし、それ以外との通信においては暗号化処理を行うような使用法が可能となる。

【０１１３】

特に、家庭とビジネス両用で携帯通信端末を用いる場合には、家庭との通信はなるべく短時間にし、ビジネス用のアクセス時間をなるべく長く取りたいといった要求も考えられる。したがって、本実施形態では、家庭との通信時に暗号化処理を省略することによって、上記の要求も満たすことが可能である。なお、情報を送信するごとに送信者が情報の機密度を通信装置に入力し、その情報の機密度を判別させるようにしても良い。

【０１１４】

また、本実施形態においては、情報送信者と情報受信者とが通信媒体としてサーバを使用しているかどうかを判別し、それによって暗号化処理の使用を決定するようにしている。例えば、サーバを介さない家庭内での情報送信では機密性が低く、さらに端末間の接続手段としてケーブルなどを使用することで盗聴の危険性も低くなる。この場合は、暗号化を行わないことによって暗号化処理に伴う負担を軽減することができ、情報送受信の高速化が可能となる。また、戸外で無線を用いてサーバを介して通信を行う場合には、盗聴の危険があるため、暗号化を行うことによって機密保持を達成することができる。

【０１１５】

さらに、本実施形態では、情報受信側が暗号化を許可しているかどうか（暗号解読が可能であるかどうか）を判別し、暗号解読が可能である場合には暗号化処理を行い、不可能である場合には暗号化処理を行わないようにしているので、送信側での暗号化処理の負担を極力軽減することができる。また、受信側の情報通信装置を暗号化処理手段を予め具備しない構造とすることもでき、受信側の情報通信装置の構造の単純化により低コスト化、小型化等を図ることができる。

【０１１６】

例えば、子供が携帯端末を持つ場合を考えると、子供の通信相手というのは親あるいは友達である場合が殆どである。子供とその親、あるいは子供同士で通信される情報の機密度はあまり高くないと考えられる。また、子供が使用するものに関しては、大人による使用の場合よりも高い耐久性が必要になるとも考えられる。さらに、携帯方法としてはポケットの中などに入れることが考えられ、子供用の小さなポケットにも入るような小型の情報通信端末が必要になる。

【０１１７】

この場合に、本実施形態の情報通信装置によれば、暗号化信号に対する受信エラー処理という簡単な機能を設けるだけで良く、より複雑な暗号化処理を省略した機能の単純化によって、装置の耐久性の向上と小型化を図ることが可能となる。さらに、情報を送信する際に、相手側が暗号化処理機能を持たない場合に暗号化処理を行わない機能を持つ情報通信装置によって、暗号化処理の最適化を図ることも可能となっている。

【０１１８】

（本発明の他の実施形態）

本発明は、上述した実施形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置に対し、上記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、その装置のＣＰＵあるいはＭＰＵに格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【０１１９】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードを装置に供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１２０】

また、装置が供給されたプログラムコードを実行することにより上述の実施形態の機能が実現されるだけでなく、そのプログラムコードが装置において稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【０１２１】

さらに、供給されたプログラムコードが装置の機能拡張ボードや装置に接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【０１２２】

【発明の効果】

本発明は上述したように、情報の通信を行う際に送信情報の暗号化手段の使用／不使用を選択する暗号処理選択手段を備えたので、暗号化処理をなるべく省略し、信号処理の負担や、暗号化に伴う処理の負担を軽減することができる。

上記暗号化処理の選択は、例えば、情報送信者からの指示に応じて暗号化手段の使用／不使用を選択することによって実現できる。

【０１２３】

また、本発明の他の特徴によれば、情報送信側の装置と情報受信側の装置とが接続されている通信媒体に応じて暗号化手段の使用／不使用を選択するようにしたので、情報送信に高い機密性が必要な通信媒体を介して情報の通信を行っている場合（例えば戸外で無線によって通信を行う場合）以外、例えば家庭内での情報送信の場合は暗号化処理を省略し、暗号化処理に伴う負担を軽減することができる。

【０１２４】

また、本発明のその他の特徴によれば、情報受信側の装置において暗号解読が可能であるかどうかの判別結果に応じて暗号化手段の使用／不使用を選択するようにしたので、受信側で暗号解読が不可能である場合には暗号化処理を行わないようにすることで、送信側での暗号化処理に伴う負担を軽減することができる。さらに、受信側の情報通信装置を暗号化手段を予め具備しない構造にすることができ、この場合には、受信側の情報通信装置の小型化、低価格化を実現することが可能となる。

【０１２５】

また、本発明のその他の特徴によれば、送信情報の機密度の判別結果に応じて

暗号化手段の使用／不使用を選択するようにしたので、高い機密性を必要とする情報を送信する場合以外では暗号化処理を省略し、暗号化処理に伴う負担を軽減することができる。

【０１２６】

また、本発明のその他の特徴によれば、受信情報が暗号化されているか否かを判別して、暗号化されていると判別された場合には所定のエラー処理を行うようにしたので、情報受信側が暗号を解読する機能を備えていない場合に、暗号化された信号を受信側に送ってしまっても、受信側ではそれを受信エラーとして対応することができるので、通信の不備に対して適切な対応をとることができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態による送信側の携帯端末と受信側の携帯端末の概略構成を示す図である。

【図２】

本実施形態による送信側携帯端末、受信側携帯端末の動作を示すフローチャートである。

【図３】

本実施形態による受信側携帯端末が暗号化処理機能を具備していた場合の受信側の動作を示すフローチャートである。

【図４】

１３９４シリアルバスを用いて構成されるネットワーク・システムの一例を示す図である。

【図５】

１３９４シリアルバスの構成要素を示す図である。

【図６】

１３９４シリアルバスにおけるアドレス空間を示す図である。

【図７】

１３９４シリアルバスのケーブルの断面図である。

【図８】

１３９４シリアルバスで採用されているデータ転送フォーマットのＤＳ－Ｌｉｎｋ符号化方式を説明するための図である。

【図９】

１３９４シリアルバスを用いて構成されるネットワーク・システムの一例を示す図である。

【図１０】

バス使用権獲得のためのアービトレーションを説明するための図である。

【図１１】

アシンクロナス転送における時間的な遷移状態を示す図である。

【図１２】

アシンクロナス転送のパケットフォーマットの例を示す図である。

【図１３】

アイソクロナス転送における時間的な遷移状態を示す図である。

【図１４】

アイソクロナス転送のパケットフォーマットの例を示す図である。

【図１５】

アイソクロナス転送とアシンクロナス転送とが混在した、バス上の転送状態の時間的な遷移の様子を示す図である。

【図１６】

バスリセットからノードＩＤ決定までの一般的なシーケンスを示すフローチャートである。

【図１７】

図１６のフローチャートのバスリセットからルート決定までの部分の手順をより詳しく示すフローチャートである。

【図１８】

図１６のフローチャートのルート決定後からＩＤ設定終了までの部分の手順をより詳しく示すフローチャートである。

【図１９】

アービトレーションの一連の流れを示すフローチャートである。

【符号の説明】

１　送信側ＰＤＡ装置（送信側携帯通信端末）

２　受信側ＰＤＡ装置（受信側携帯通信端末）

３　情報処理部

４　暗号処理選択部

５　暗号化信号処理部

６　情報送受信部

７　情報処理部

８　受信エラー処理部

９　情報送受信部

１０　受信エラー表示部

ｄ１　情報信号

ｄ２　暗号化信号

ｄ３　暗号化請求信号

ｄ４　受信エラーメッセージ信号

ｄ５　送信者からの暗号化要求信号

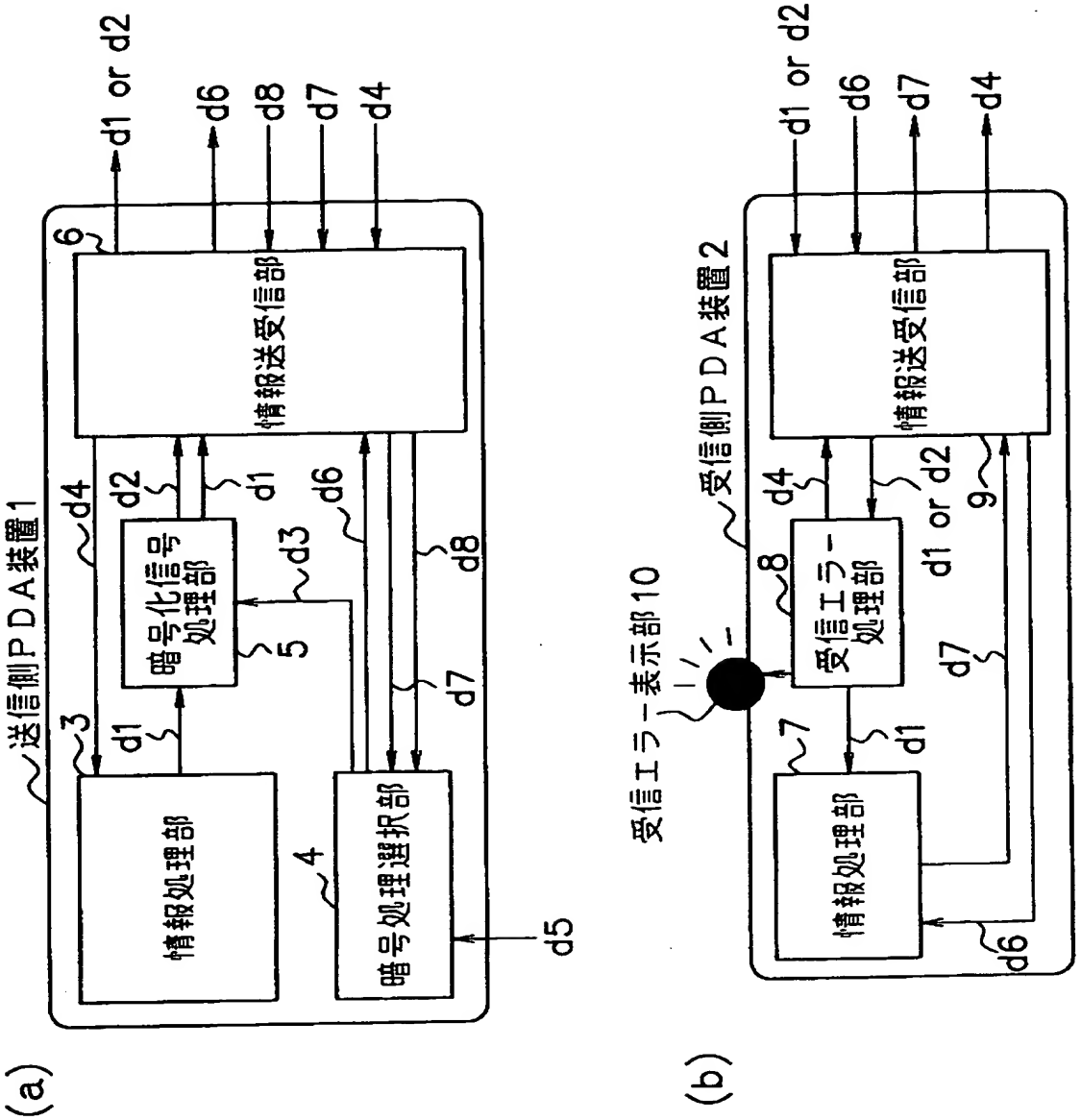
ｄ６　暗号化許可の判定請求信号

ｄ７　暗号化許可信号（内容は不可）

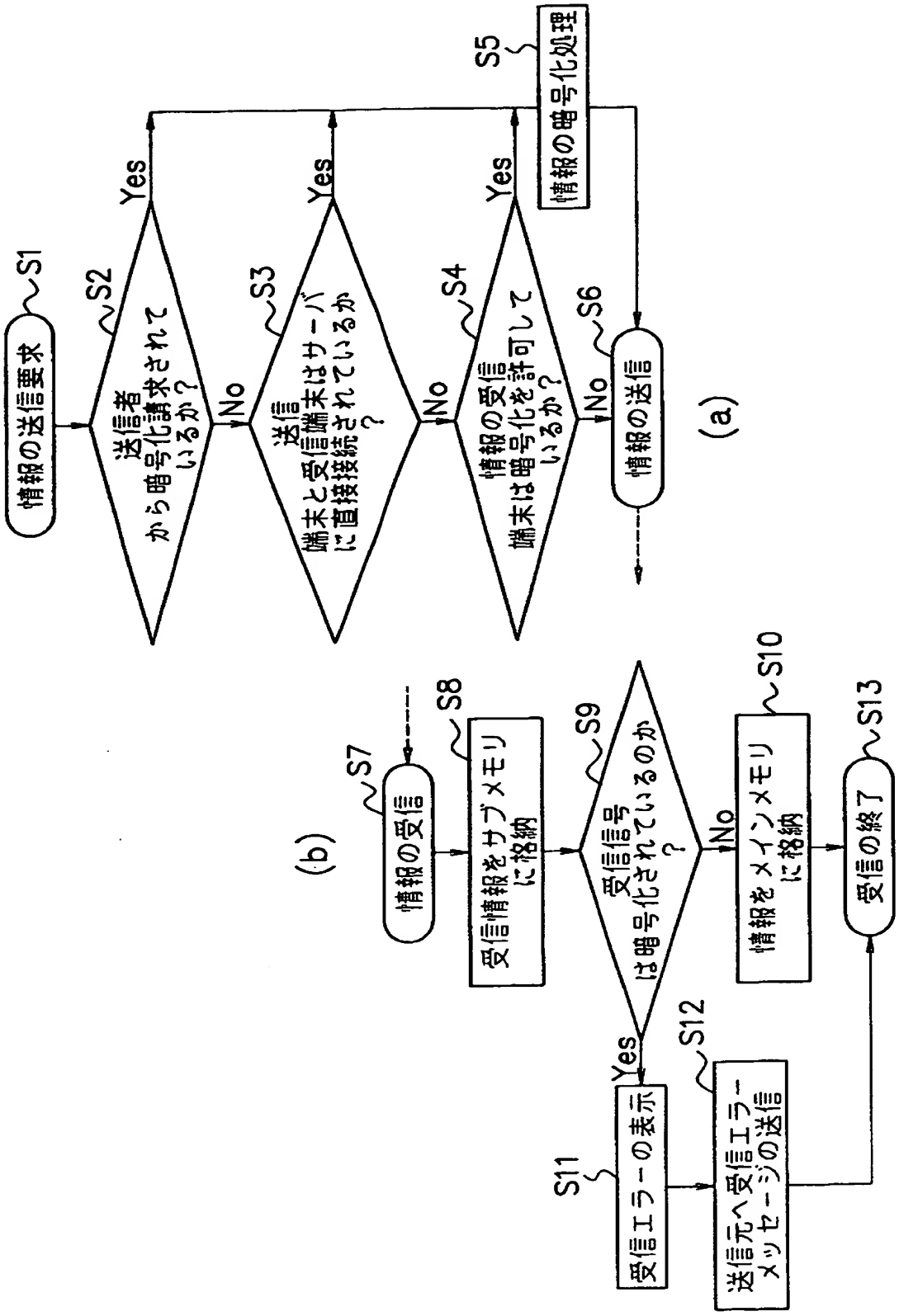
ｄ８　サーバからの携帯通信端末の接続状況信号

【書類名】　図面

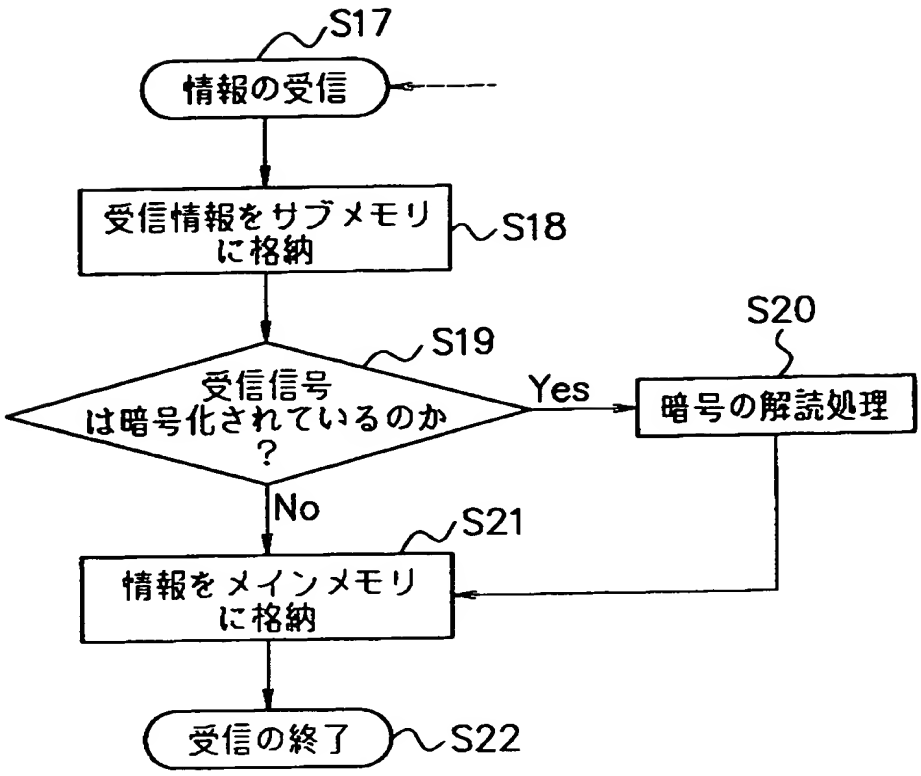
【図１】


(a)
送信側ＰＤＡ装置1
情報処理部
暗号化信号処理部
暗号処理選択部
情報送受信部
d1 or d2
d6
d8
d7
d4
d5
(b)
受信側ＰＤＡ装置2
受信エラー表示部10
受信エラー処理部
情報処理部
情報送受信部

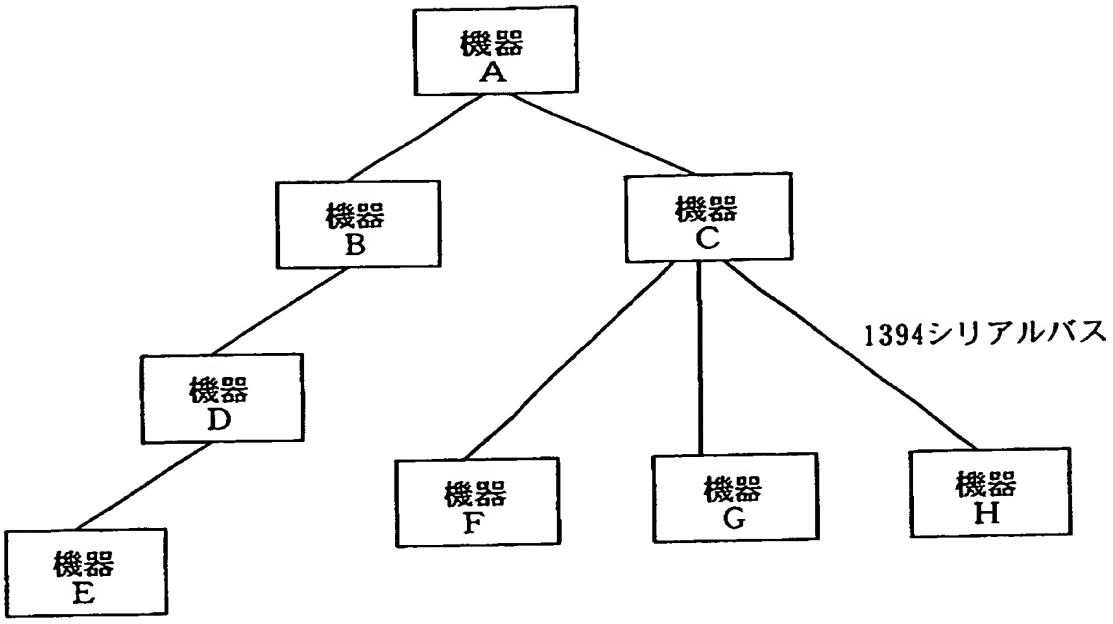
【図２】


(a)
情報の送信要求
S1
S2
送信者から暗号化請求されているか？
Yes
No
S3
送信端末はサーバに直接接続されているか？
Yes
No
S4
情報の受信端末は暗号化を許可しているか？
Yes
No
S5
情報の暗号化処理
S6
情報の送信
(b)
S7
情報の受信
S8
受信情報をサブメモリに格納
S9
受信信号は暗号化されているか？
Yes
No
S10
情報をメインメモリに格納
S11
受信エラーの表示
S12
送信元へ受信エラーメッセージの送信
S13
受信の終了

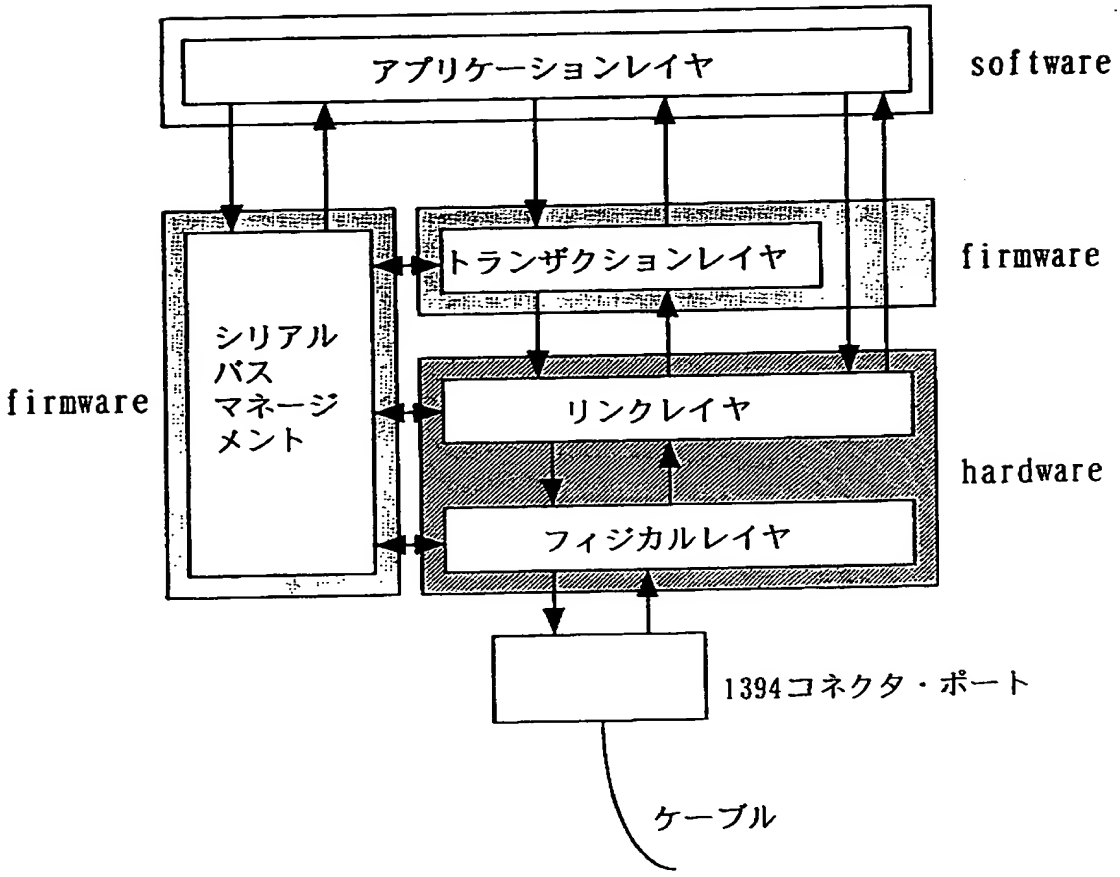
【図３】


S17
情報の受信
受信情報をサブメモリに格納
S18
S19
受信信号は暗号化されているのか？
Yes
S20
暗号の解読処理
No
S21
情報をメインメモリに格納
受信の終了
S22

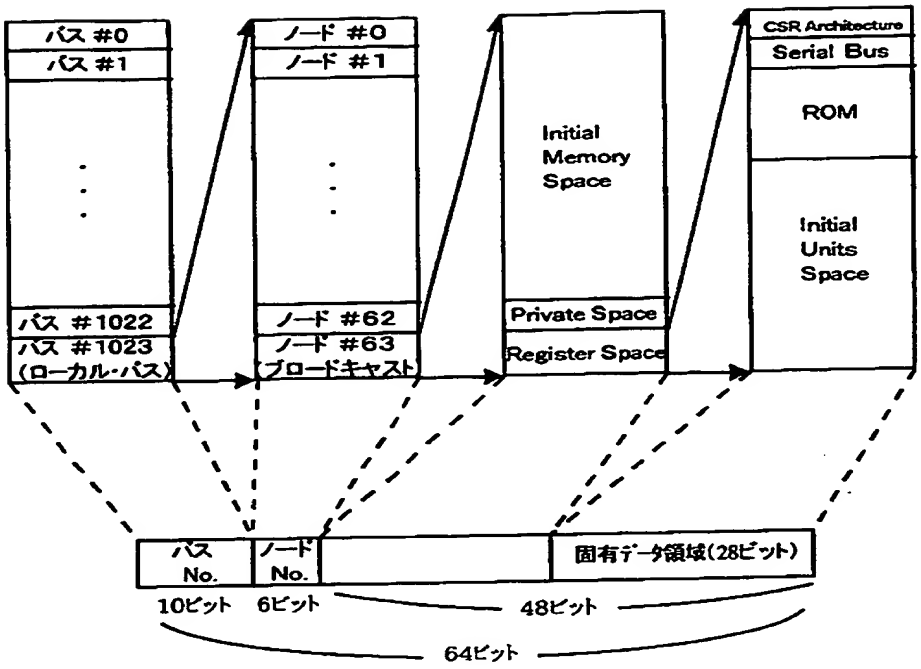
【図４】



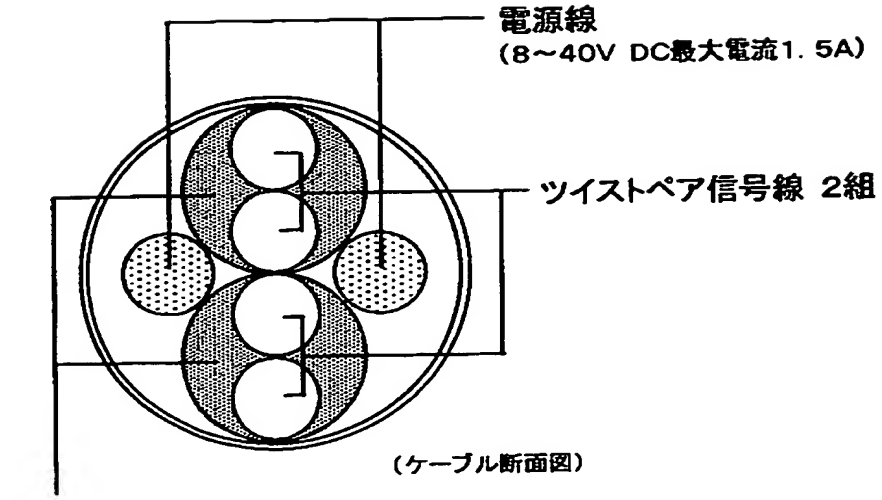
【図５】


アプリケーションレイヤ
software
トランザクションレイヤ
firmware
シリアル
バス
マネージ
メント
firmware
リンクレイヤ
hardware
フィジカルレイヤ
1394コネクタ・ポート
ケーブル

【図６】

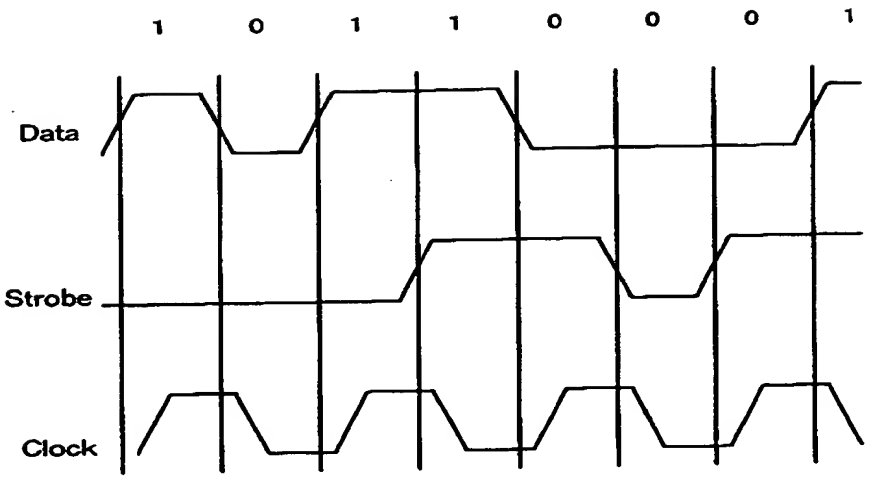

バス #0
バス #1
バス #1022
バス #1023
(ローカル・バス)
ノード #0
ノード #1
ノード #62
ノード #63
(ブロードキャスト)
Initial
Memory
Space
Private Space
Register Space
CSR Architecture
Serial Bus
ROM
Initial
Units
Space
バス
No.
ノード
No.
固有データ領域(28ビット)
10ビット
6ビット
48ビット
64ビット

【図７】



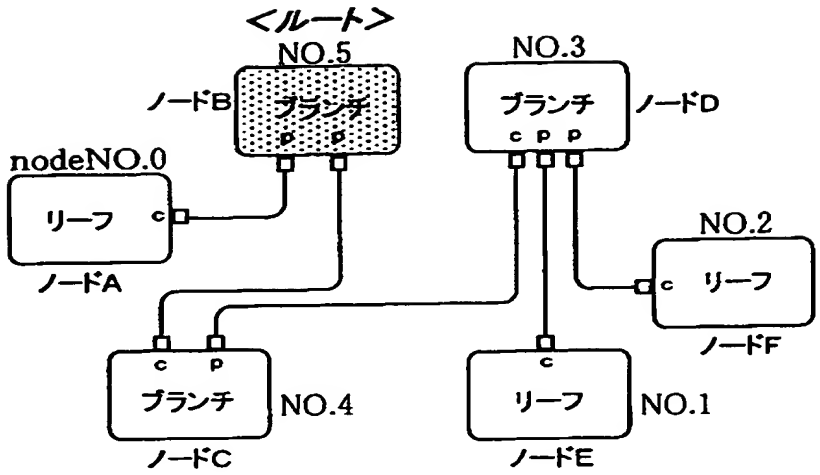
(ケーブル断面図)

【図８】



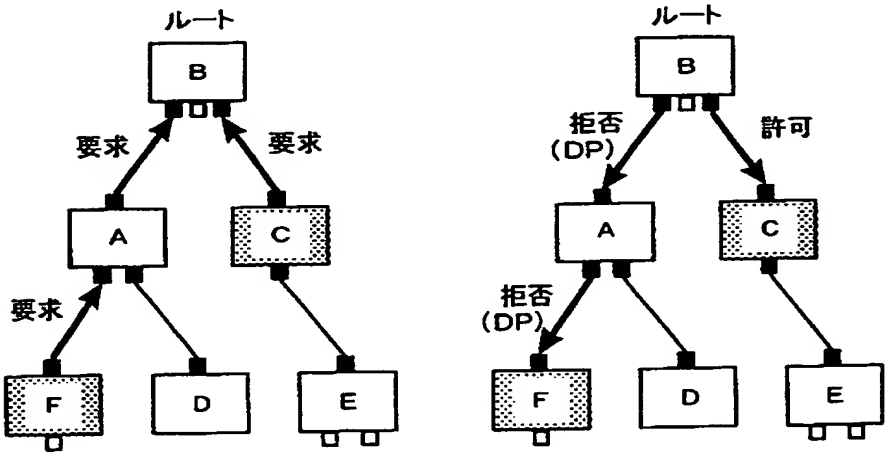
（DataとStrobeの排他的論理和信号）

【図９】



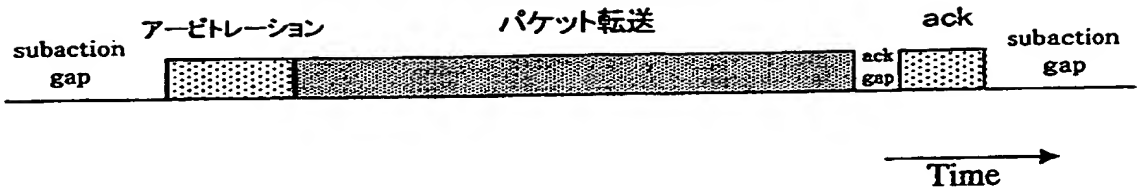
□:ポート
ブランチ:2つ以上のノード接続があるノード　c:子のノードに相当するポート
リーフ　:1つのポートのみ接続があるノード　p:親のノードに相当するポート

【図１０】

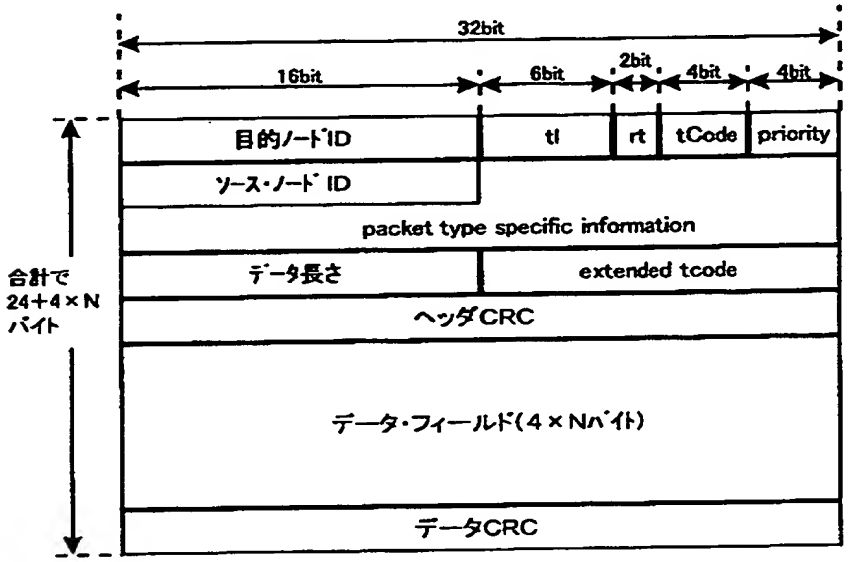


(a) バス使用権の要求　　(b) バス使用の許可

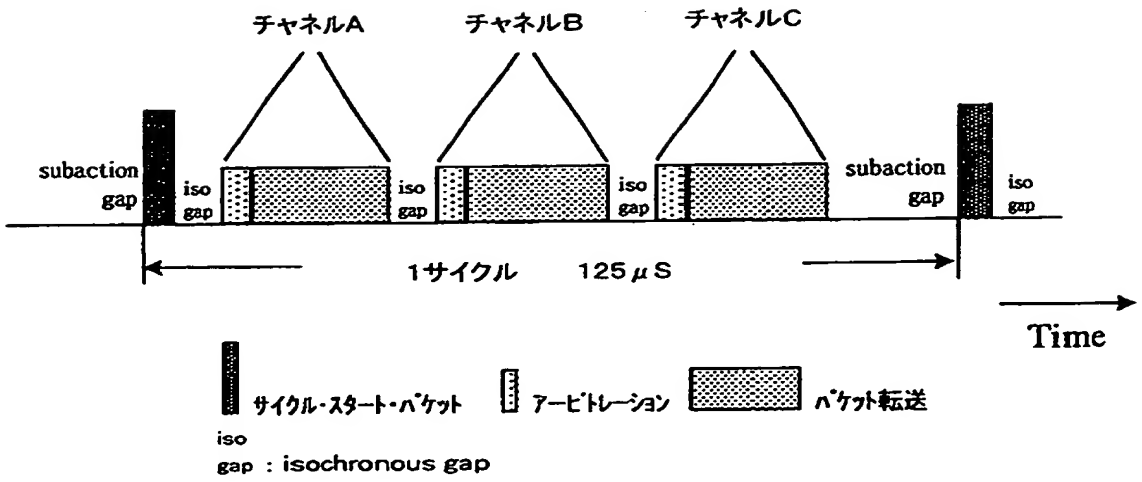
【図１１】


subaction gap
アービトレーション
パケット転送
ack
ack gap
subaction gap
Time

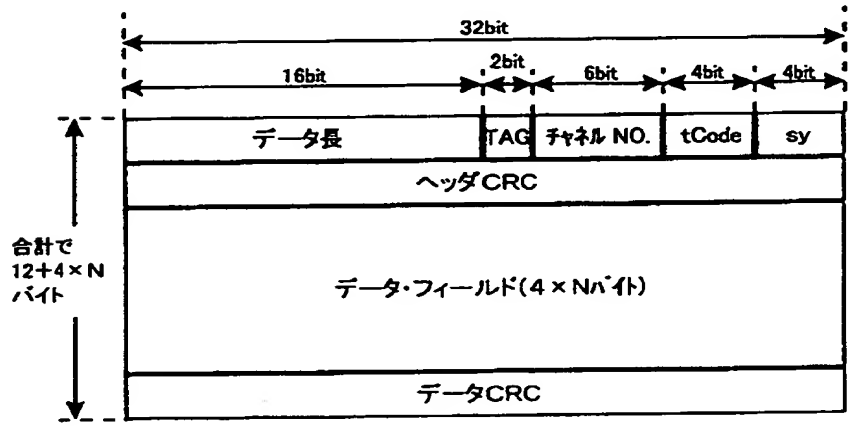
【図１２】


32bit
16bit
6bit
2bit
4bit
4bit
目的ノードID
tl
rt
tCode
priority
ソース・ノードID
packet type specific information
データ長さ
extended tcode
ヘッダCRC
データ・フィールド(4×Nバイト)
データCRC
合計で
24+4×N
バイト

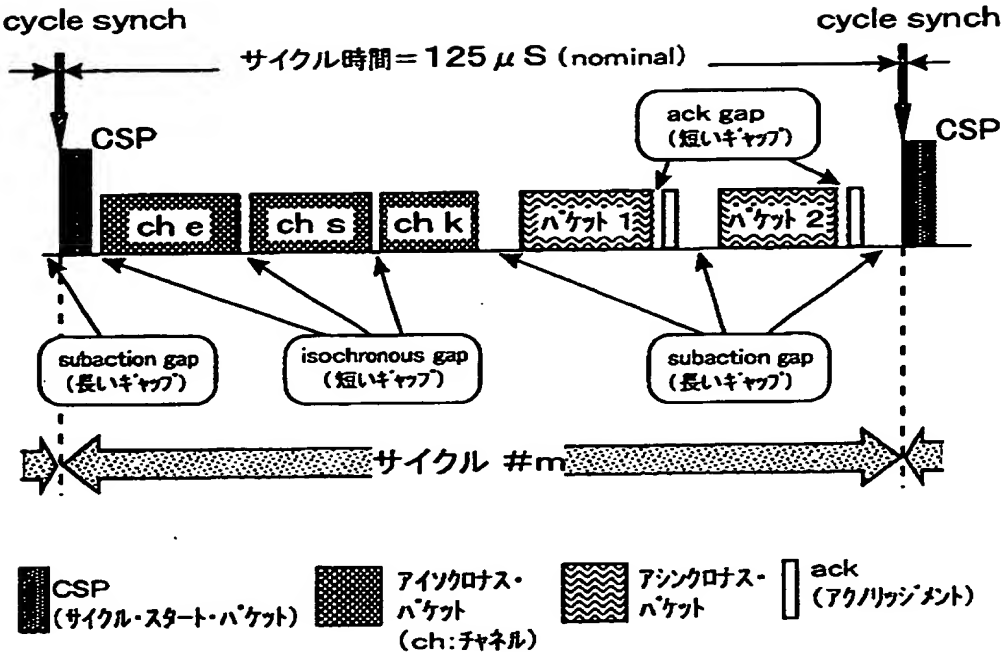
【図１３】


チャネルA
チャネルB
チャネルC
subaction gap
iso gap
iso gap
iso gap
subaction gap
iso gap
1サイクル　125μS
Time
サイクル・スタート・パケット
アービトレーション
パケット転送
iso gap : isochronous gap

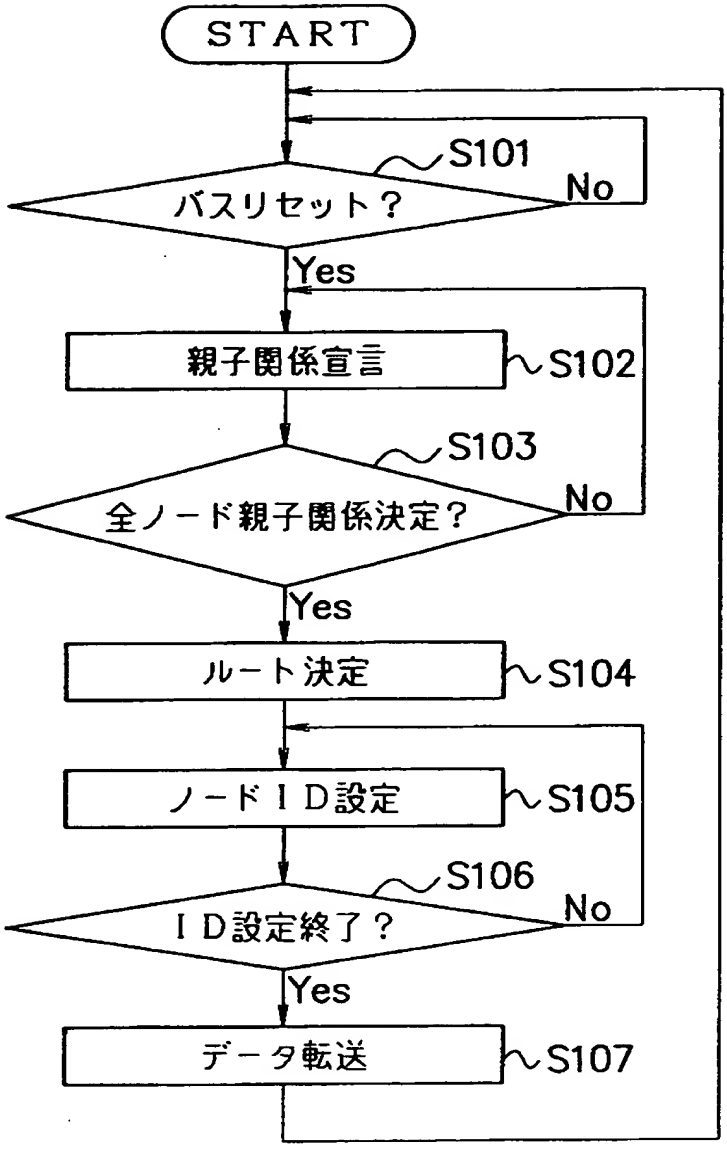
【図１４】


32bit
16bit
2bit
6bit
4bit
4bit
データ長
TAG
チャネル NO.
tCode
sy
ヘッダCRC
データ・フィールド(4×Nバイト)
データCRC
合計で 12+4×N バイト

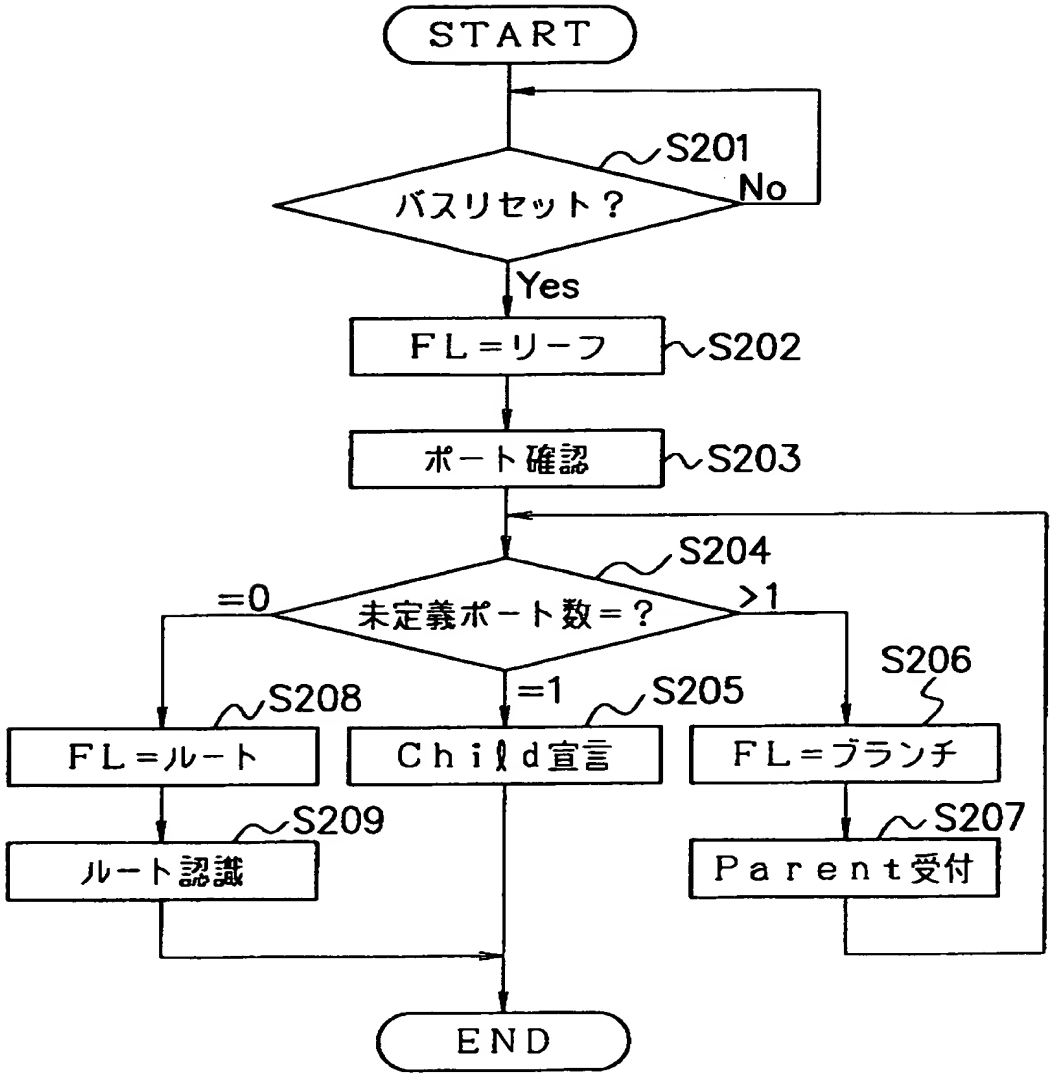
【図１５】


cycle synch
cycle synch
サイクル時間＝125μS (nominal)
CSP
CSP
ack gap
(短いギャップ)
ch e
ch s
ch k
パケット 1
パケット 2
subaction gap
(長いギャップ)
isochronous gap
(短いギャップ)
subaction gap
(長いギャップ)
サイクル #m
CSP
(サイクル・スタート・パケット)
アイソクロナス・
パケット
(ch:チャネル)
アシンクロナス・
パケット
ack
(アクノリッジメント)

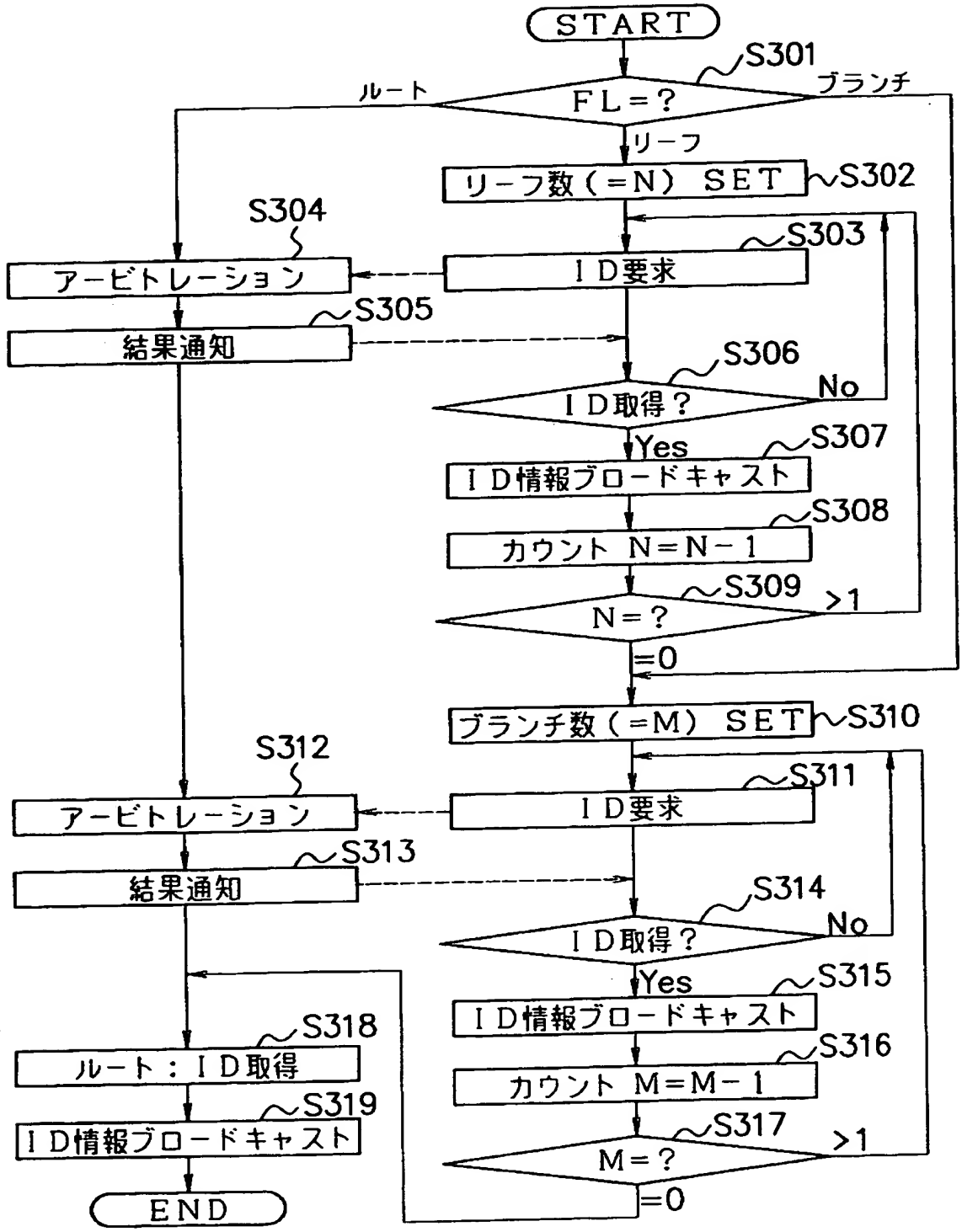
【図１６】


START
S101
バスリセット？
No
Yes
親子関係宣言
S102
S103
全ノード親子関係決定？
No
Yes
ルート決定
S104
ノードＩＤ設定
S105
S106
ＩＤ設定終了？
No
Yes
データ転送
S107

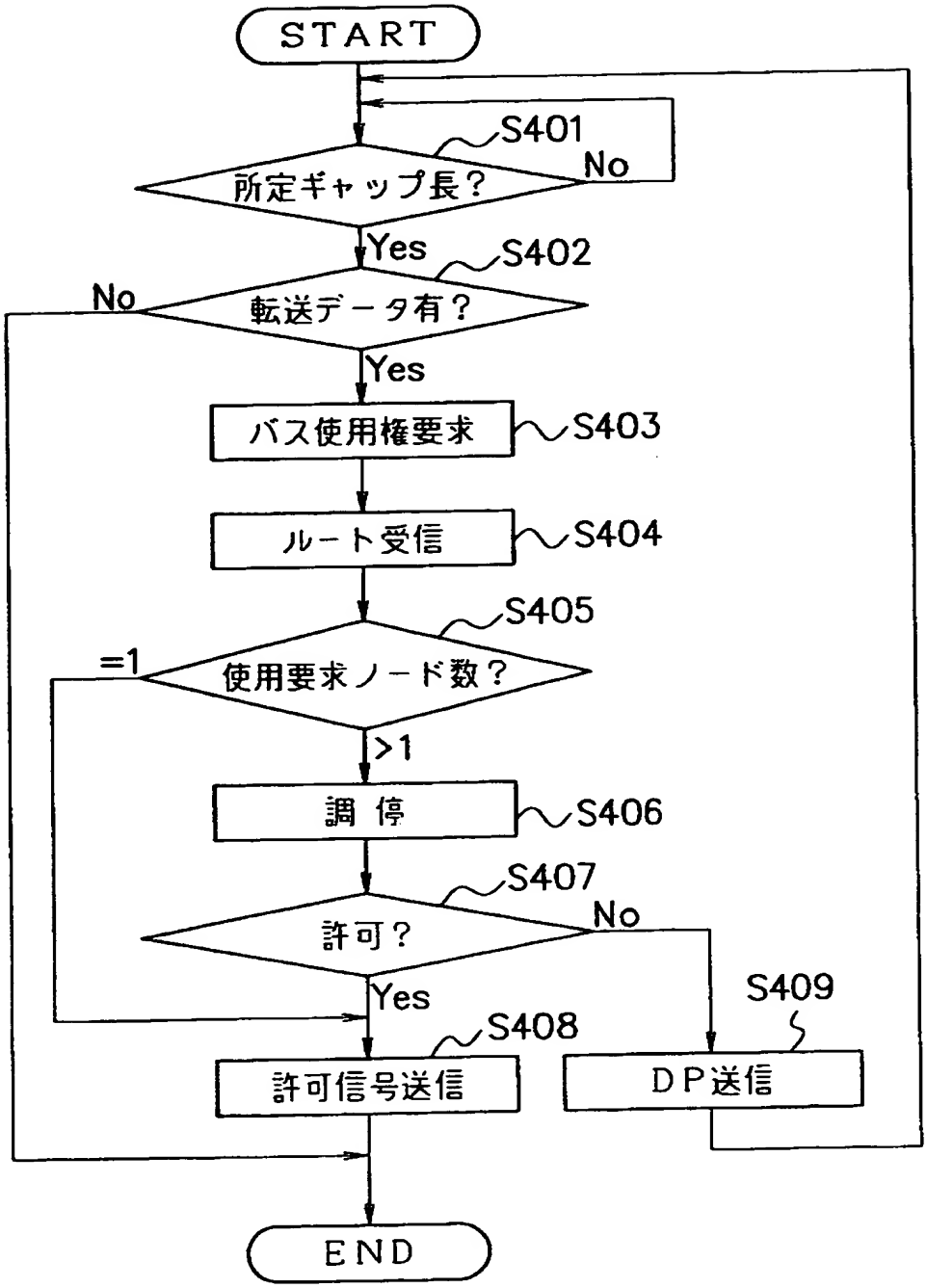
【図１７】


START
S201
バスリセット？
No
Yes
ＦＬ＝リーフ
S202
ポート確認
S203
S204
未定義ポート数＝？
=0
=1
>1
S206
S208
S205
ＦＬ＝ルート
Ｃｈｉｌｄ宣言
ＦＬ＝ブランチ
S209
S207
ルート認識
Ｐａｒｅｎｔ受付
END

【図１８】


START
S301
FL＝？
ルート
ブランチ
リーフ
リーフ数（＝N） SET
S302
S304
S303
アービトレーション
ＩＤ要求
S305
結果通知
S306
ＩＤ取得？
No
Yes
S307
ＩＤ情報ブロードキャスト
S308
カウント N＝N－１
S309
N＝？
>1
=0
ブランチ数（＝M） SET
S310
S312
S311
アービトレーション
ＩＤ要求
S313
結果通知
S314
ＩＤ取得？
No
Yes
S315
ＩＤ情報ブロードキャスト
S316
カウント M＝M－１
S317
M＝？
>1
=0
S318
ルート：ＩＤ取得
S319
ＩＤ情報ブロードキャスト
END

【図１９】


START
S401
所定ギャップ長？
No
Yes
S402
転送データ有？
No
Yes
バス使用権要求
S403
ルート受信
S404
S405
使用要求ノード数？
=1
>1
調 停
S406
S407
許可？
No
Yes
S409
S408
許可信号送信
DP送信
END

【書類名】　　要約書

【要約】

【課題】　情報の暗号化処理を考慮しつつも通信携帯端末の小型化、低価格化、情報処理の負担減を実現できるようにする。

【解決手段】　送信情報の暗号化を行う暗号化信号処理部５と、情報の通信を行う際に暗号化信号処理部５の使用／不使用を選択する暗号処理選択部４とを設け、送信情報の暗号化処理を実行するか否かを必要に応じて選択できるようにすることにより、暗号化処理をなるべく省略し、暗号化に伴う処理の負担を軽減できるようにする。また、例えば、情報受信側において暗号解読が可能である場合には暗号化処理を行い、不可能である場合には暗号化処理を行わないようにすることで、受信側の情報通信装置を暗号化処理手段を予め具備しない構造とすることができるようにして、受信側の情報通信装置の低コスト化、小型化等を図る。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000001007
【住所又は居所】　東京都大田区下丸子３丁目３０番２号
【氏名又は名称】　キヤノン株式会社
【代理人】　申請人
【識別番号】　100090273
【住所又は居所】　東京都豊島区東池袋１丁目１７番８号　池袋ＴＧホーメストビル５階　國分特許事務所
【氏名又は名称】　國分　孝悦

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社